UNIVERSITY OF CALIFORNIA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

OFFICE OF THE PRESIDENT

Robert C. Dynes
President

1111 Franklin Street
Oakland, California 94607-5200
Phone: (510) 987-9074
Fax: (510) 987-9086
http://www.ucop.edu

April 20, 2004

Mr. Alan Dechert
Open Voting Consortium
9560 Windrose Lane
Granite Bay, California 95746

Dear Mr. Dechert:

Thank you for your letter of February 16. I appreciated learning more about the Open Voting Consortium's plan to submit a proposal to the Secretary of State for a voting modernization project designed to help the State implement the federal Help America Vote Act of 2002. Improving the mechanisms for voting in order to ensure an accurate, trustworthy, and cost-effective system is a worthy goal. I am pleased that you are working with University of California researchers who can lend their expertise to this important project.

I appreciate your invitation to join you in urging the Secretary to fund this proposal. Unfortunately, I cannot be involved personally in advocating for funding the myriad good proposals submitted by UC researchers. It would be more appropriate for you to work directly with the University of California researchers who are collaborating with you on this proposal. Since they are the experts who will be serving as Principal Investigators on the project, they are in the best position to answer questions that may arise about the proposed research.

The University of California is fortunate to count among its faculty many researchers with extensive knowledge in public policy, political science, and computer science. If you would like to identify additional UC faculty with expertise in areas related to voting modernization, please get in touch with Lawrence B. Coleman, Vice Provost for Research. He would be happy to assist you, and he can be reached at (510) 987-9436.

Thank you for letting me know about your work. I have no doubt that UC researchers can make great contributions to this area, and I wish you the best of luck with your efforts.

Sincerely,

Robert C. Dynes

cc: Provost Greenwood
Vice Provost Coleman

Posted on Thu, Apr. 08, 2004

The touch-screen holy grail

E-VOTE PROTOTYPE HAS RIGHT STUFF

Mercury News Editorial

An electronic voting system that's cheap, secure, accurate and easy to use. One that uses off-the-shelf hardware and publicly examinable software. One that voters can trust.

A prototype of such a system -- the holy grail of election officials -- was on display last week in San Jose. It looked like the real deal.

Had the federal government underwritten the research behind it years ago, such a system might now be making its debut in voting booths. Instead, the demonstration took place in a conference room at the county government building with its creators in search of financial backers and government grants.

The government unwisely ceded development of electronic voting machinery to private companies like Diebold Voting Systems, whose proprietary software is under electronic lock and key. The secrecy of the source code, a slew of malfunctions, and a lack of a paper copy that voters can look at have eroded confidence in touch-screen voting.

The founders of Open Voting Consortium, a non-profit group of software engineers and computer scientists, built the system in their spare time. It features open-source software, which means that the public can examine the software code to make sure there are no bugs or digital shenanigans built in. It also produces a paper version of the ballot cast, converted to a bar code, so that voters can privately verify that the choices they made on a touch-screen are just as they intended.

California Secretary of State Kevin Shelley has mandated a voter-verifiable trail in all counties by 2006, but so far, the big voting-machine companies are not marketing machines that do that.

Open Voting Consortium's system has appeared too late for Santa Clara and other counties that have been plunking down tens of millions of dollars for touch-screens that lack some of the new system's virtues. But many counties that weren't under pressure to replace equipment have put off the decision, for good reason. For them, this next generation of voting systems may be worth the wait -- if not too long.

Open Voting Consortium appears to have what it takes to inspire faith in electronic voting. Its system can't come to market soon enough.

THE VOTER CERTIFIED BALLOT

The Proposal and Reference Materials
Prepared for the Sacramento County Registrar of Voters' Office and the Secretary of State's Office

By Alan Dechert
February 13, 2001

Some of the topics,

The Voter Certified Ballot

A Proposal for Ballot Reform by Alan Dechert

February 13, 2001

Revision History: Dec. 12, '00 - Jan. 17, '01: various refinements including focusing on making it a PC-based system. The January 17th version was distributed to quite a few interested parties.
Feb 13, '01: two sections added, namely, the section on "The ATM Model" and the section on "Potential Vote Fraud." Other details added include,

- *Making the computer code Open Source (freely available)*
- *Development of production software to be included in the study.*
- *System certification to be included in the study.*
- *More detail on the paper ballot alternative procedure*

Introduction

This is a proposal to take the first step toward implementing a new system for casting and counting ballots. More specifically, this proposal is for a detailed study of how to implement the Voter Certified Ballot system on a trial basis in one county (or voting district) in California for the 2002 election. This new ballot system utilizes an off-the-shelf PC for each voting booth. Other features of the system are discussed here.

Clearly, we deserve a tighter system for casting ballots and counting ballots. A nation-wide system probably cannot be mandated--without a Constitutional amendment anyway. Despite the obstacles, something must be done. There is no excuse for tolerating such a badly flawed system in light of all the low-cost technology that is now available.

If a good workable system can be demonstrated in one state, then it can be replicated elsewhere. A countywide demonstration could be a precursor to statewide implementation. Effective vote system reform can be implemented without federal involvement.

While the debacle in Florida underscored the problem, this could have happened in most any state. Ballot problems were put under a magnifying glass due to the pivotal vote count there.

In Florida, there was a wide variety of procedures, machinery, and ballot styles in use--all with a built-in rate of error higher than we'd like to see and certainly too high to reliably count the vote in an election so close. The same could be said of the procedures, machinery, and ballot styles used in most every other state.

Our voting system misrepresents the truth. Look at the results of any election. The numbers are presented as if accurate to within one vote. According to the World Almanac, Bill Clinton got 47,401,185 votes in 1996. What chance is there that this figure represents the number of voters that left the polling placing believing they had cast a vote for Clinton? If the truth were told, it would go something like this:

> This number represents a summation of counts that come from a vast assortment of election officials where a great variety of methods, procedures, ballot types, ballot marking equipment, and ballot counting machines were used. This number is certainly incorrect and may be off by as much as one percent or more. The voter has no way to verify how his or her vote was counted or if it was counted at all. There is also no way for the voter to verify any of the counts reported. There are always many ballots that have an "overvote" or "undervote" where there exists

a legal vote that was not counted due to machine error, voter error, or some other problem. We know that these facts do not inspire confidence in the system.

Usually, more than half of the people eligible to vote stay away from the polls. It is unknown how many of those would have voted (or how they would have voted) if they had more confidence in the system.

Is it possible that in some future election each and every ballot could be counted accurately? Many people think so, or believe we could come very close to this level of accuracy. Most proposals promising greater accuracy involve deployment of some type of electronic system or systems.

As we move away from the clumsy, inaccurate, fraud-prone manual systems, inexorably toward more computerization, we are also opening the possibility for fraud on a scale never before imagined. All sorts of tricks are possible for manipulating electronic data. We've seen many clever but malicious tricks with computers. No doubt, we'll see even more of them in the future. We must keep this in mind before adopting any new system.

The system described here addresses many of the weaknesses in current and proposed systems. While I generally agree that the Internet cannot be relied upon for a total solution, I think it can and should be part of the solution. The paper trail must remain due to all the reliability and security issues related to computer-based voting. I recommend that the voter certify his or her own vote at the polling place with a paper copy showing how the vote was counted.

All ballot systems in use or proposed have the same weakness: they all ask the voter to trust the election officials too much. The voter must trust that his or her ballot will be handled correctly. The voter must trust that the equipment used to count the ballots is neither "rigged" in any way nor otherwise deficient. The voter has no way to verify anything.

This proposal introduces a new concept: The Voter Certified Ballot ("VCB"). With this system, the voter certifies that his or her ballot gets recorded correctly. In the end, the voter can certify that it was counted correctly. No manipulation of the vote can be hidden.

Some issues such as voter file maintenance and absentee ballot procedures are only mentioned here. This proposal mainly addresses polling place procedures and ballot handling and counting. These are the most critically deficient areas. Voter file maintenance is an on-going process and I feel the Secretary of State is making good progress in this area.

In my earlier drafts of this document, I assumed that pre-printed ballots would continue to be the preferred way for voters to indicate preferences. I showed how the Voter Certified Ballot system could be applied to a variety of data input systems. I started by talking mostly about working with the pre-printed ballot. After much debate, I've concluded that it will likely be simpler, more secure, more flexible (including accommodating visually impaired voters), and cheaper to abandon the pre-printed ballot. So, I changed my emphasis here to demonstrate how a PC-based Voter Certified Ballot would work, while mentioning ways the VCB could be implemented using other equipment.

I. Description of Hardware Setup

A standalone PC and printer will be set up in each voting booth. The CPU and keyboard will be inaccessible to the voter: only the mouse, monitor and printer will be within reach (the keyboard should be unplugged--removed altogether from the PC). The mouse will be a very simple one-button mouse so that people not familiar with PCs will not get confused by multiple buttons, wheels, and so on.

The PCs could come from existing inventories of government agencies, businesses, or individuals. Most any modern PC setup (including printer) will do.

Additional hardware configurations will be devised to accommodate vision-impaired voters. Also, by utilizing a touch-screen monitor (or touch-screen overlay on a standard monitor) voters that may lack sufficient eye-hand coordination to operate the standard setup can indicate preferences by simply pointing with a finger. If implemented, this system would most likely include one PC set up for the vision-impaired, another PC set up with a touch-screen monitor, and several other PCs with a configuration (with mouse) that most voters will be comfortable with.

II. Main Features and Benefits of Proposed System

1. Ballot reading issues resolved. Voter certifies machine reading of ballot before leaving polling place.
2. Overvotes not possible.
3. Traditional strengths of current system retained such as personal identification at the polling place and ballot anonymity.
4. Enhance access to democratic system by making detailed precinct-by-precinct voting data publicly available on the Internet.
5. Increase voter participation by proving that each vote gets counted accurately.
6. Robust and redundant. Simple, secure, accurate, resistant to computer failures.
7. Fast and accurate vote counts available within minutes of poll closing.
8. Recount results will reproduce totals with 100% accuracy.
9. Vote is counted and certified by the individual voter and precinct pollworkers before ballots are transported anywhere.
10. Ability to accommodate voters not wanting to use electronic system by offering a paper ballot if needed.
11. Low cost. Almost no new dedicated voting equipment to purchase.
12. Greater community involvement in the process.
13. Much better ability to accommodate vision-impaired voters.
14. Improved ability to meet requirements for ballots in different languages.
15. Write-in votes counted accurately and automatically.

III. The ATM Model

In a December 14 press release, "The presidents of MIT and Caltech have announced a collaborative project to develop an easy-to-use, reliable, affordable and secure United States voting machine that will prevent a recurrence of the problems that threatened the 2000 presidential election."
They go on to say,

> "Beware of the assumption that newer technology is more complicated. The trend is the opposite," said Dr. Vest. "Most people have been able to figure out ATMs. That's our model," remarked Dr. Baltimore.

While the VCB system has been developed independent of the Caltech/MIT project, I largely agree with the ideas and principles laid out in their press release. In particular, I think the ATM model is instructive.

With the exception of the Voter Certified Ballot system, there is an important attribute of ATMs totally lacking in voting systems: Verification of the transaction comes in two parts, namely, (1) a printout upon completion and (2) a bank statement where the transaction appears and can be reconciled with the beginning balance, the ending balance, and all the other transactions.

Both parts are required. Can you imagine your reaction if your bank informed you that they would continue to provide the receipts but would no longer make available detailed statements of all your transactions? Suppose they said, "If your balance shows less than you think it should be, it's probably because you made some transactions you didn't record or forgot about. We're not going to give you any detailed listing you can check against." We wouldn't accept this and we shouldn't accept anything like this from our election officials either.

Another observation about ATMs: Often, people don't save their receipts or even when they do save them they don't do anything with them. We often see the area around the ATM littered with receipts--a lot of

them are in the waste basket nearest the machine. Some gas stations have addressed this problem by making the printed receipt an option. Perhaps a voting system that provides a receipt should also offer an option not to print one.

Our confidence in using ATMs is enhanced by having this two-part verification, whether we choose to reconcile our statements with the receipts or not. If either part were denied to us, we would have less confidence in ATMs. The receipts would be particularly useless if there were no detailed statements to check against.

In some places, ATM-like touch-screen voting systems have been used where the voter gets no receipt and no statement showing where and how the vote was counted. This is analagous to using an ATM and being told by the bank to trust that the transaction will be handled properly, while not providing a receipt or any other way for the user to verify that it was handled correctly. We would not accept this from our bank and we should not accept this from election officials.

The Voter Certified Ballot system provides the two-part verification, similar to what we get with our ATM transactions. And, like ATMs, it offers voters the speed, convenience, ease-of-use, and accuracy lacking in other systems.

IV. Potential Vote Fraud

Most of the experts that have looked at the Voter Certified Ballot system have objected to giving the voter the ballot copy on the grounds that it would lead to vote buying. I believe they are mistaken. Here are four of the main reasons that they are mistaken on this subject:

1. Most of the examples they use (when direct vote buying was a significant problem) date from the 19th century. The conditions that exist today are much different and those examples are not relevant. The electronic age makes this type of fraud very risky and not profitable. With hidden cameras, hidden microphones, and so on, the vote buyer is at risk for a sting operation and/or blackmail. The electronic age also means that dollars that might have worked to buy votes can be better spent through radio, TV, and the Internet to gain votes.
2. If this type of direct vote buying were so attractive, we'd see more of it today. If proof of how one voted were such valuable information, it would be easy to hand a voter a small digital camera (or scanner) and instruct the voter to make a copy while in the booth. Upon returning the camera with the image as proof, the vote buyer could then complete the transaction.
   We don't see this type of fraud because it's too risky and too convoluted. Any similar fraud using the ballot copy offered in the VCB system would be equally convoluted and risky.
3. It is widely known that absentee ballots open all sorts of possibilities for fraud. This type of vote buying would be much easier with absentee ballots than with the VCB system. If it were such a big problem, we'd have much stricter restrictions on absentee voting. As it is, the State of California makes absentee ballots available to any voter with no reason needed.
4. The ballot copy offered with the VCB system would be worthless to a potential vote buyer. It provides no proof at all. The voter knows that the copy is authentic but the buyer would have no way to verify this since copies could be easily forged. Election officials can authenticate the ballot due to embedded information but without the key used to create the embedded information, no one else could tell the difference between the real copy and a forgery.

V. Proposed Procedures for the Voter

Voters will check-in at the polling place and the pollworker will find their name in the preprinted logbook ("roster") prepared for the precinct. The pollworker will put a check mark next to the voter's name. The voter will not sign in at this time and will not receive a ballot or anything else.

After entering the voting booth, the voter will find a standard PC monitor displaying the ballot application that is running. There will be a large button on the screen that says "BEGIN" (along with translations of "begin" in all the languages that need to be supported). When the user clicks this button, the next screen enables the user to select a different language. After that, the voter is presented with a screen showing the

first items on the ballot with check boxes next to them. A "Next" button will appear at the bottom of the screen indicating they should go to the next screen after making selections.

On the next page, the voter will see a "Go Back" button on the bottom as well as the "Next" button (assuming there is another page). Upon reaching the last page, there will be a button that says something like, "Click here when you have made all your selections." After clicking on this button, a preview of their printed ballot is displayed. At the bottom of the ballot preview, there are two buttons: "Go back and change my ballot" and "I'm finished. Print it!" When finished, a unique ballot number is generated and recorded electronically along with the voter's selections. Two copies of the ballot are printed with the ballot number and precinct number printed on each corner.

Options will be available to enter write-in candidates. If selected, a screen will pop-up with an on-screen keyboard which can be used to spell out the name of the candidate.

As the voter makes choices, those choices will show up very clearly with each selection brightly highlighted. For example, when the voter first sees a list of candidates for a particular office, each name will be displayed clearly; once the voter makes a selection, the name will appear brightly highlighted with a large check mark next to it while the other names will be greyed and barely readable. All the candidates' names will return to the original display if the voter deselects his or her choice. It will be easy an obvious to select or deselect any item.

The printouts will utilize a font that can be easily read by machines and by people.

After the voter clicks on the print button, a message appears that says:

> Check the accuracy of your ballot. Your anonymous vote has been recorded electronically but the printout you are receiving now will be used to resolve any discrepancies.
>
> **Do not make any marks of any kind on the ballot!** If anything on the ballot does not look right to you, you should start over. If it looks like a printer problem, tear up the ballot and report this the problem to a pollworker. Then go to another voting booth and start over.
>
> When you are satisfied that the ballot reflects your intended vote, place both copies face down in the privacy folder. Go to the pollworker, deposit your ballot, and sign-out on the logbook. One copy will be handed back to you: the other will be dropped into the ballot box.

The very last screen would say, "Do you want to print a copy of your ballot to keep for your reference?" There would be a large "Yes" button and a large "No" button (the default in case the voter does not respond would be "Yes"). At the bottom of this screen would be a message, "Unless you specify 'No,' a reference copy will be printed in x seconds" (where x represents a count-down in seconds beginning with, say, 5.

The printout would say something like "Undervoted" for any item on which the voter made no selection. Overvotes are prevented by the software.

As soon as the voter completes the process, the electronic file will be resorted by ballot number so that no one could later identify a particular voter's ballot by keeping track of the order of the users of the PC.

VI. Implications for Pollworkers

Pollworkers will have to learn a few new concepts and procedures. None of these would be very demanding. Little or no familiarity with computers would be required for most pollworkers. There would need to be at least one pollworker available capable of setting up and running a standard PC.

The certified printout becomes the authentic document. It is the actual ballot. This settles all issues related to whether or not the machine read the ballot correctly.

The electronic record of the vote (from which the printout was produced) is a simple one line ASCII text database record (fixed length or variable length delimited, to be determined).

The record has the fields as indicated before, i.e.

1. ballot number
2. state (2 char abbreviation)
3. county
4. precinct number
5. Y/N indication for first ballot item
6. .
7. .
8. .

... Y/N indication for last ballot item
write-in candidate 1
write-in candidate 2
....

If more than one precinct votes at a single polling place, partitions should be used such that the equipment would record the correct precinct for the voter. It would be possible for voters from different precincts to use the identical voting equipment but this would complicate matters under this design. In this case, when the voter checks-in, the pollworker would need to direct the voter to use one of the PCs. Also, the pollworker would need to verify the precinct number (by turning up the corner of the ballot) upon accepting the ballot from the voter (unless the pollworker observed that the voter used the correct booth).

After the polls close, the pollworkers must count the ballots and verify that the number of ballots matches the number of signatures.

VII. Copying the Results From Each Precinct

When the polls close, the electronic records of the votes are merged into a single text file. A pollworker accomplishes this by rebooting each voting-booth PC and bringing up the ballot program in administrator mode. The program has a "Copy data to floppy disk" menu item. After all the files have been copied to diskette (or possibly other media), the diskette is taken to another PC to consolidate the data. The electronic file is sorted by ballot number and printed out. The number of electronic records must match the number of signatures and the number of ballots.

However, it's possible there will be other spurious records due to mistakes or mischief. All "extras" must be deleted from the file and the list reprinted. When the printed list has the correct list of ballots, the workers verify the data. One person reads aloud from each ballot while several others with copies of the printed list check them off. A technical note here: the spurious records would not be physically deleted--"suppressed" might be a better characterization. The records identified as spurious would not show up in any tally. The spurious records would be retained in case a voter later produced a copy of a ballot that they claim was never counted. In this case, the error can be proven as a voter error (that is, the voter must have printed another ballot but turned in the "wrong" one).

Under this scheme, every county maintains a web site and makes space available to each precinct. Domains are created for each precinct. The domain-naming scheme might go like this:

http://www.st-county-precinctnumber.gov

So, http://www.ca-santaclara-2419.gov would belong to precinct 2419 in Santa Clara county, CA. After the pollworkers have certified that the file is correct, they post the file to their domain. The name of the file would simply be votedate.txt so each precinct would have posted 20001107.txt to their own domain if this system had been in place this year. The raw text file is available to anyone but a script on the server would

also be run to display the data in a browser-readable easily comprehensible table with headers (indicated the contents of each column).

Once all the files from all the precincts are copied to the county server, tallying the vote does not depend on Internet access since all the data would be on the same computer. The totals should be available in a matter of seconds.

VIII. Certifying the Result

Currently, ballots are not normally read at the precinct level. The pollworkers only count the number of ballots, not the markings on the ballot. The ballots are transported to a more centralized location where they are processed. While this means that the votes can be counted in a more controlled environment, it also has some drawbacks.

1. The ballots are put at risk in the process of transporting them before anyone knows what's on them. While this process is normally orderly and careful, historically, there have been problems and there is no guarantee similar problems will not occur in the future.
2. It is too slow. People want to know the results. There is no excuse for not being able to deliver a quick and accurate count after the polls close (if a national election, results should not be posted until the polls close in all time zones). Right now, the officials can't deliver the counts right after the polls close because the ballots are on the road somewhere. When they do arrive at their destination, they must wait in line with the ballots from many other precincts before they are counted.

With the VCB, there are several layers of certification. First, the voter certifies his or her own ballot. Second, the pollworkers at the precinct certify that the file transmitted to the county (and posted on the county web site) is accurate. Beyond that, there are procedures for the county to certify the accuracy of the counts.

Once the precinct workers copy the data to their Internet site, the system administrator for the county locks out all users from accessing the data. The precinct workers re-examine their data on the Internet and certify that it is correct.

The county would certify the count using several techniques. After the pollworkers have finished their work, the ballots get transported to wherever election officials normally take ballots. As part of the certification process, some or all of the ballots will be scanned and the results automatically compared with the results posted by pollworkers at the precincts. Probably, it will not be necessary to scan all the ballots: a few samples from each precinct might be adequate.

A list of all precincts in the county would be available from the county's web site. In addition, at this point, ANYONE can count the vote as a crosscheck. The voter could import the data for his or her precinct into any spreadsheet or database program and verify the totals that election officials have posted for the precinct. Also, a simple script could roll through the entire precinct domains for any given county and accumulate to totals on any bargain basement PC connected to the Internet. This has the additional benefit that valuable voting pattern information previously available only to organizations with the resources to buy the data would now be freely available to anyone that can get on the Internet. The text files remain on the Internet indefinitely and serve as a resource for research.

While the final certification of a statewide election would remain with the Secretary of State, each individual voter can verify that their vote was counted and that it was counted correctly.

IX. Touch Screen Voting

Touch Screen Voting may prove to be the ultimate way to go but it's not clear if the advantages would outweigh the high initial costs. It certainly is worth investigating. While avoiding the cost of a pre-printed ballot and the cost of reading the ballot, each voting booth would have to be outfitted with relatively expensive equipment. In order for touch screen voting to work, the machine must be blind to the actual voter identity.

If the cost can be justified, the voting procedure could work similar to the PC-based VCB system described above. However, it is felt that since most voters will be comfortable using a mouse, it will be difficult to justify the cost of making a touch-screen system standard for all votes cast at the polling place.

X. Vision Impaired Voters

The PC-based VCB system makes it quite feasible to accommodate people that don't see well or at all. A totally blind person could vote utilizing a special version of the ballot software that works with a headphone instead of a monitor. The blind voter would be prompted by a recorded voice. "Click the mouse button to begin." "Click the right mouse button to vote for xyz. Click the left mouse button if you don't want xyz." After the click, on to the next item. At the end, selections are read to the voter for verification and a procedure for changing is included. The printout would be handled the same way. Even though the voter couldn't read it while in the booth, someone else assisting the voter could read it later (or they could elect not to print one).

For people that are not blind but have difficulty seeing, they may be helped by the use of extra large fonts on the screen and on their ballot. Or they could use the headphone system for the blind.

Any system(s) set up for the blind should also be usable for sighted voters. If a system were set up for their exclusive use, it could compromise voter anonymity if, say, only one voter used the system on election day.

XI. Procuring the PCs

The county would maintain a web page called something like "PC Lenders Signup." This page would have a list of all precincts and there would be two buttons next to each precinct number. One would say "Map" (which would lead to a graphic display showing the location of the precinct). The other would say "Lenders Signup."

Selecting the Lenders Signup button would lead to a list of people and the machines offered for Election Day, and would have a form to fill to add more. There would be instructions there something like this:

> Please sign up even if it appears there are an adequate number of PCs pledged for this precinct--we may need some backups! All modern Apple-type or IBM-type PCs can be used. Enter your name, organization (if applicable), processor (for example, Athlon), speed (for example, 850), RAM, harddrive, printer make and model [and so on] and the number of units matching this description you are willing to lend for Election Day.
>
> We can only accept whole setups except for the mouse (which we will supply) that are known to work. We need to have the CPU (with CD ROM drive and a diskette drive), monitor, keyboard, printer, and all cables necessary to hook it up. Your PC will not be connected to a network.
>
> You will need to arrange for delivery (at least 24 hours before polls open) and pickup of the equipment (within 24 hours after the polls close). In addition, you will need to sign a waiver absolving the county of any loss that you may incur due to this program. You will be given a receipt including serial numbers of all equipment you bring in. Every effort will be made to handle your equipment properly but we make no guarantees.
>
> You will be responsible for backing up and restoring your harddrive since all programs and data will be erased before we install the ballot program. You need to show proof that you own a valid license for the operating system we use.

Immediately after you sign up, send an email to PCLendersProgram@OurCounty.gov and include your name, address, and phone number. We will contact you.

Clearly, this program would involve some time, trouble, and risk for the PC lenders. Whether or not sufficient numbers of usable PCs could be obtained in this way remains a fair question. This is one of the gating issues to be studied.

A basic assumption of this proposal is that lenders would accrue goodwill by supporting "progress in democracy" with "support for modernization of the ballot process." Public acknowledgement of lenders should remain published on the Internet for some months after the election. Other incentives may be promoted as required (for example, stickers, thank you letters from the Secretary of State, etc.).

XII. Software Requirements for the PC-Based VCB

One of the main tasks to be completed before implementing this system involves development of a simple and robust software program for creating the ballot. This software would be installed along with the operating system and would be the only application running. After the PC boots, in "administrator mode." After login, the administrator can select several options:

- PC Number
- Load data
- Precinct Number
- Install printer
- Copy voters' ballot data to disk
  etc...

In this design (the PCs are not networked), the PC number would be a critical piece of data. The ballot software would produce a unique ballot number for each voter in the precinct. It would be a random number selected from a range of numbers. In order to ensure uniqueness, the ranges for the various PCs used must not overlap. So, for example, PC number one would select ballot numbers from 1000 to 1999, PC number two would select ballot numbers from 2000 to 2999, and so on. Once a ballot is printed using a PC, the PC number cannot be re-used. That is, if the PC broke down and was replaced while the polls were open, care must be taken to ensure that the replacement doesn't use the same number or any other number already used.

The Load data option is to load the information provided by election officials that is supposed to be on the ballot. This means that the software can be used for any future elections by importing the election data file. In other words, the specific options being voted on would never be hard-code.

A disk image would be created and burned onto many CDs for each district (each area that has the same options on the ballot). Setting up a PC for a given precinct would involve booting to the CD and copying the image (operating system and ballot application) to the harddrive. Upon bootup, the setup person enters the PC number and the precinct number, and installs the printer. Then, s/he enters "voter mode" and tests to make sure it all works. After the test, the test data would be erased.

XIII. Security Issues

This system is inherently resistant to vote fraud due to all the crosschecks. No manipulation of the vote can be hidden. The voter gets a copy of the completed ballot and then can verify it was counted since each vote is published on the Internet.

However, it seems reasonable to assume that some will attack the system if for no other reason than to create mischief. For example, someone could try to throw a monkey wrench into the system by forging a ballot, which they bring to the polling place and substitute for a ballot produced there. This would create a situation where a ballot exists with no corresponding electronic record. The VCB system expects to have some electronic records with no corresponding printed ballot (for example, due to the voter starting over after printing one already, or starting over due to print failure). However, there should be no way to have a

ballot with no electronic record. Such a forgery should be easy to spot given that the exact format of the output will be nearly impossible to replicate.

In addition, check marks could be included on the printed ballot that would be spaced apart according to a cipher applied to the ballot number. This cipher would be unique to the PC with the only record of it entered in a logbook on Election Day. The contents of the cipher would be unknown to anyone in the precinct (the keys would be kept in a secure location by county or state election officials) so it would be impossible to know the correct spacing between the check marks without having access to the keys. This extra step may or may not be needed since it only provides one method to prove a forgery. Forgeries are not likely to be prevalent since they provide no advantage to the voter and will only cause their vote to be thrown out. Further study of potential forgeries might be useful.

While the PCs would be under observation by pollworkers on Election Day, there is some risk of tampering between the time the PCs are set up and configured (with the software they will use on Election Day) and when the polls open. Software would be included to authenticate the boot up procedure and ensure the right operating system and right ballot software gets loaded when the PCs are started on Election Day.

Procedures could be in place so that the machines could be used while networked or without a network connection. For the sake of security and simplicity, I do not recommend networking the PCs.

This system will be somewhat more vulnerable to power outages than non-electronic systems. At a minimum, it is likely that an uninterruptible power supply should be installed to ensure that votes in the process of writing to the database could be completed. It might be desirable to make a small electric generator available to operate in case of an extended power outage. This problem is not unique to the VCB system: Any electronic voting system would have similar vulnerabilities. It would be worthwhile to examine procedures already in place to deal with power outages at traditional polling places. Further study of this issue would be done in the feasibility study that would follow acceptance of this proposal.

The ballot software will log to disk all selections by the voter until the vote is completely recorded to the database. In the event the power plug of the PC is pulled, the software should be able to restart automatically and pick up where it left off as soon as power is restored.

Procedures would need to be developed for dealing with machine breakdowns, paper jams, etc. A secure system for posting results from the precincts to the county maintained web domains would be needed. Also, a procedure would be included for pollworkers to manually recreate the electronic record from the printed ballot in an instance where the data file on a given PC was somehow damaged or lost and could not be recovered (anticipated to be very rare, but it is possible).

XIV. Costs

The PC-based Voter Certified Ballot system would be very cheap. After the initial setup and training costs required for the first election, it should be much cheaper than traditional systems: No ballots to print, almost no voting equipment to purchase, store, and depreciate.
The cost for voting equipment would be small but might include mice and touch-screen overlays. In addition, there would be some cost for polling place furniture--tables, partitions, curtains, and so on. Estimates will be developed as part of the study.

While PC-based VCB system would be the ultimate in cheap once established, there would be significant startup costs. Mostly these costs would involve development of software, development of procedures, training, and a public relations campaign to inform voters about the new system.

If the VCB system were used with a preprinted ballot, it would not be so cheap but the cost might be justified. At least one machine would be required for each precinct to accept the original ballot and print the certified copy. The ballot reading machinery would be the main new piece of hardware required. With full PC setups (including scanner and printer) commonly available for less than one thousand dollars, these machines should not cost more than this since they will consist of basically the same components. Several might be required for each polling place.

Touch screen voting would require purchasing a higher number of units (one for each voting booth) but may turn out to be cost-effective. The first implementation of this design would have a high cost-per-unit. Mass-produced, per unit hardware and software costs would be expected to drop significantly.

XV. Absentee Ballots

A remaining issue has to do with the absentee ballots. I recommend that they always get counted and always get posted to the Internet just like the normal votes. I would suggest they have a ballot number that would also denote that they were absentee. It may be impractical to give the voter an opportunity to review how the ballot was read before it is officially counted.

I believe that usually absentee ballots are blindly separated from the envelopes before they are processed. It might be possible to preserve voter anonymity and give the absentee voter an opportunity to see how the vote was counted. This could be done by incorporating a tear-off envelope with the absentee ballot that contains the ballot number (or the voter could manually record the number from the ballot).

Absentee ballots always involve some compromise of voter anonymity. Voter anonymity is supposed to be protected by procedures followed by election officials and the people working on their behalf. However, unlike voting at the poll, these procedures cannot be personally witnessed by the voter.

Another alternative might be to have the absentee voter go to some institution where s/he has an established relationship (like a bank) so that identity can be verified and a ballot number issued. The voter could go to a PC connected to the Internet and follow much the same procedure followed in a voting booth as described previously for the PC-based VCB system. The difference would be that the voter would mail-in one copy of the ballot (instead of handing it to the pollworker). Upon receipt of the ballot, the election official would verify the ballot number then erase the ballot number from the record connecting that number to the individual. Admittedly, this is a compromise but may be no worse than existing procedures for absentee ballots.

XVI. Internet Voting

While certain aspects of this proposal involve the Internet, overall, this is *not* a proposal to implement Internet voting and I adamantly oppose any proposal intended to enable remote Internet users to vote via the Internet en masse. The only instance where Internet voting might deserve serious consideration would be the absentee voter procedure previously discussed.

XVII. Possible Voter Disenfranchisement

The vast majority of voters will readily accept the PC-Based Voter Certified Ballot system because PCs have become reliable tools they use on a regular basis. However, it is anticipated that a small percentage of voters will react negatively to the new system. Some people will "never trust computers" or will simply be uncomfortable using one.

As quoted earlier, Dr. Baltimore of Caltech said, "Most people have been able to figure out ATMs." However, banks don't force people to use them. People can still function perfectly well without ATMs and can enjoy the personal assistance from a teller if they so choose.

As with any new ballot system, care must be taken not to disenfranchise any voters. A ballot for manual marking could be printed for voters not wanting to use the new system (printed on-the-spot with a function of the ballot software, letter or tabloid size).

After marking the paper ballot, the voter would return to the pollworker and the pollworker would ask, "Will you wait for a receipt?" The manually marked ballot could be given to another pollworker who would enter the selections at the PC and generate the completed ballot. In order to preserve secrecy of the ballot, the pollworker making the entries would be in another room or behind a partition and not within earshot of the voter.

The hand-marked ballot would then have the computer-generated ballot number manually recorded on it. The hand-marked ballot would be folded-in and placed in the privacy folder with the two copies of the finished ballot placed face-down on top of the hand-marked ballot.

The pollworker doing the data entry would hand the folder back to the first pollworker who would return to the voter (if the voter has decided to wait for the receipt). The pollworker would then ask the voter, "Would you like to verify that your ballot has been recorded correctly?" (show the voter back to the voting booth to review the ballot copies).

Most likely, the voter will return to the pollworker and say, "It's correct" or something like that. If not, the pollworker would ask, "Did you mark your corrections?" If so, the pollworker tears up (or puts them in a shredder) the printed copies and takes it back to the entry person to redo. The old ballot number is crossed out and the new one recorded.

It's possible that the voter will still have problems, perhaps claiming, "I want to vote for both candidates" or claiming that the ballot is still not right. These cases should be rare and pollworkers would need some training on how to handle these situations gracefully.

Once the pollworker has the hand-marked ballot along with voter-approved ballot copies, the printed copies are handled like all the rest and the voter signs out on the roster. The hand-marked ballots are stored separately where they may be used later for verification.

This type of ballot handling represents some compromises and extra work, but it is anticipated that the number of such cases will be small and will decrease as the electorate continues to become familiar with the system and continues to become familiar with PCs in general.

XVIII. Implementing the PC-Based Voter Certified Ballot

This system may be the cheapest and best system yet devised. If so, it could become the de facto standard all over the United States while satisfying the requirements for worthwhile ballot reform.
Several steps must be taken before that can happen. Upon acceptance of this proposal, resources would need to be allocated in order to develop a detailed implementation plan (call it "feasibility study," "study," or just "plan").

This is a bottom-up approach (as opposed to top-down). A top-down approach is probably not feasible due to the decentralized nature of voting system decision-making.
Broadly speaking, there are six steps:

1. Develop a plan to implement the system in one county (or voting district(s)).
2. Execute the plan (after approval and funding obtained).
3. Wrap up documentation and make it available so that it may be followed easily by others.
4. Implement the system in multiple counties and voting district in subsequent elections.
5. Implement the system in multiple states in subsequent elections.
6. Nation-wide acceptance.

The plan (step 1) would cover many topics including,

- Identify key players and tasks
- Identify a geographical area for the pilot project and obtain all the necessary commitments of political support and cooperation.
- Identify and describe in detail all the other tasks to be performed
- Identify possible changes that might be needed in election law (for example, we might need to make it illegal to force anyone to reveal their ballot number).
- Develop a budget for the pilot project.
- Identify funding source(s) to satisfy the budget requirements.
- Outline Public Relations campaign to inform voters of new system--gauge receptivity.
- Conduct surveys and publish results.

- Set up and maintain a website (preferably on the Registrar of Voters page) where all details will be published
- Identify specific makes and models of PCs that will work with the system (Apple may not be supported in first implementation of the system)
- Describe how an adequate number of usable PCs can be obtained for Election Day.
- Outline training program for people involved in setting up polling places.
- Document polling place set up procedures.
- Create a polling place mock-up and recruit volunteers to test procedures.
- Design polling place equipment to accommodate the PCs (tables, partitions, curtains, etc. and get cost estimates)
- Describe how the new system will interface with the old.
- Investigate the utility of including an option for an explicit undervote (i.e., "none of the above")
- Describe in more detail how absentee ballots and provisional ballots would work with this system.
- Address vulnerability to power outages and other security issues.
- Gather information on other voting systems that have used some of the features of the VCB (I have an unconfirmed report that Brazil used PCs in their national election; Also, I've heard that receipts have been issued in some demonstration systems, e.g., LA County in the early 1990s)
- Develop a list of milestones with dates along with criteria for making go/no-go decisions. The last milestone will clearly delineate all the conditions that must be met in order to obtain final go ahead.
- A fallback plan to mothball the new system and go with the old system in case the final milestone conditions cannot be met.
- Develop prototype ballot software.
- Develop specification for production ballot software.
- Develop a test plan for testing the ballot software.
- Complete the production ballot software, including testing.
- Obtain certification for the system.

XIX. Conclusion

If this system can be implemented successfully countywide, it could be implemented statewide in later elections. The state could accumulate the vote from the counties much the same as the county would accumulate votes from the precincts in the system described here.

Voter anonymity is preserved since only the ballot number is given in the electronic database. The voter retains the only record linking the ballot number with the specific voter.

This system has multiple levels of verification to ensure an authentic and accurate vote count. Not the least of which is the fact the voter would go home with a printout of their vote and can, at any time, log on to the Internet and verify that their own vote has been posted and is correct.

We can and should demand end-to-end verification. The voter's printout is a good step. But it's only part of the puzzle. It's possible to devise a system where you give the voter a printout of the vote that exactly represents the selections made, while writing the data to the database according to whatever formula the programmer wants to use! Some might feel that publishing the vote in the way I am suggesting is overkill. Actually, it should be considered an absolute requirement for any large-scale implementation of computerized voting.

The VCB system could be implemented with any variety of voting equipment. The main requirement is the ability to produce the electronic file representing the voters' selections. The PC-based VCB system makes use of the great number of PCs out there (and under-utilized).

The PC-based Voter Certified Ballot has been designed for voter ease-of-use. While it should prove very easy and simple for voters, there is some complexity involved behind the scenes. There are many

difficulties to be worked out having to do with procedures, methods, software, and training. Once accomplished, this knowledge can be reused and reapplied anywhere.

The pilot program proposed here could potentially work out all these details. The geographical area chosen for the pilot program must be sufficiently large and diverse so that it will represent a real world test.

Alan Dechert,
4700 Allegretto Way, Granite Bay, CA 95746
adechert@aol.com
916-791-0456

Text from Dec 14 Press Release
http://www.caltech.edu/events/mitcit/citmit.html

Caltech and MIT Join Forces to Create Reliable, Uniform Voting System

The presidents of MIT and Caltech have announced a collaborative project to develop an easy-to-use, reliable, affordable and secure United States voting machine that will prevent a recurrence of the problems that threatened the 2000 presidential election.

The announcement was made in a joint video news conferences at MIT and Caltech Dec 14.
"It is embarrassing to America when technology fails and puts democracy to such a test as it did this month," said Caltech President David Baltimore, who opened the hour-long live teleconference in Pasadena, California.
"Academic institutions have a responsibility to help repair the voting process so that we don't see anything like this again. This project is intended to protect the system from the problems we've seen in the last election," Dr. Baltimore said.
MIT President Charles M. Vest, speaking from Cambridge, echoed Dr. Baltimore's concern for the security and credibility of the voting process.
"We must find a solution. Each of us must be confident that his or her vote has been reliably recorded and counted. A country that has put a man on the moon and an ATM machine on every corner has no excuse," said Dr. Vest.
"America needs a uniform balloting procedure. This has become painfully obvious in the current national election, but the issue is deeper and broader than one series of events," said Vest and Baltimore in a Dec. 12 letter to President Vartan Gregorian of Carnegie Corporation of New York.
Gregorian said, "I want to congratulate the two presidents of our nation's most distinguished universities for their leadership in this welcome and timely initiative on behalf of our election system. Voting is the fundamental safeguard of our democracy and we have the technological power to ensure that every person's vote does count. MIT and Caltech have assembled a team of America's top technology and political science scholars to deal with an issue no voter wants ignored. This research is certain to ensure that America's voting process is strengthened." Gregorian said he will recommend the Carnegie Corporation board fund the $250,000 initial phase of the research.
The grant will be used by a team of professors from each university who are experts in technology, design and political science. The team members include Massachusetts Institute of Technology Professors Stephen Ansolabehere of political science and Nicholas Negroponte, chairman of the MIT Media Lab; and Caltech Professors Thomas Palfrey of political science and economics; Jehoshua Bruck of computation and neural systems and electrical engineering; and R. Michael Alvarez, associate professor of political science.
LESSEN CONFUSION
Professor Ansolabehere, speaking at the teleconference, said, "We are going to consider voting technologies from the paper ballots of the nineteenth century to the latest. First, we'll look, literally, at what people do in the voting booth. There, our goal is to lower voter confusion.
" Second, we'll look at how votes are counted, comparing the precinct level to a central counting agency. We will look at the strengths and weaknesses of voting technologies, find the greatest weakness and work from there. Our goal is to find the most reliable among existing technologies."
The first phase of the joint project - surveying existing technologies and setting up criteria -- would be complete in about six months, Professor Ansolabehere added.
Professor Palfrey of Caltech noted there were "issues that didn't hit the press in Florida but that are critical, including comparing the cost of existing technologies to the cost of standardization and modernization, which could run into several billions of dollars.
"But compare that one-time cost to the $300 billion annual defense budget. It's a small price to pay for modernizing democracy," he said.
Professor Palfrey also noted other issues for the MIT-Caltech team to explore, such as the impact of the current system of election administration, which is "highly decentralized and fragmented," and the role of

absentee voting, with its implied concerns of security, liability, privacy, maintenance and software development.

FEEDBACK

Professor Negroponte, chairman of the MIT Media Lab, spoke to his bi-coastal colleagues and the media about the actual interface between people and any voting machine.

"Whatever is invented will include some interface with machines, whether we vote by computer, paper or in a voting booth. The Media Lab intends to make that interface as easy as possible," he said.

Professor Negroponte outlined the goals of the joint project from the perspective of design and feedback by comparing the act of voting with the act of pushing a button to summon an elevator.

"Right now, there's no feedback at all in voting. You push the button. Nothing happens. It's like when you push the elevator button and nothing happens: you don't know if the elevator is broken or the light is broken. It would be good to have some degree of feedback in voting. For example, you might get some feedback saying, 'you voted for x,'" he noted.

ATM THE MODEL

The MIT-Caltech faculty team took a generally lighthearted view of the alleged challenges to the public of mastering new voting technology, despite months of media attention to voter confusion over the various forms of ballots and punch-card machines that didn't punch.

"Beware of the assumption that newer technology is more complicated. The trend is the opposite," said Dr. Vest. "Most people have been able to figure out ATMs. That's our model," remarked Dr. Baltimore.

Subj: Re: MIT/Caltech Uniform Voting System Study
Date: 1/31/01 10:06:40 AM Pacific Standard Time
From: Adechert
To: sda@MIT.EDU (Stephen Ansolabehere)

In a message dated 1/31/01 9:18:42 AM Pacific Standard Time, sda@MIT.EDU writes:

> You should first check that your system is legal.
>

Thanks for your prompt reply, Stephen. I will look into that some more. I don't believe it is illegal primarily because I've discussed it with quite a few knowledgeable people who would know that and surely point that out it (if it was illegal).

I agree that most experts think it would be a bad idea to give the voter a copy of the ballot. I don't buy it. Many of those that think it would be a bad idea also make reference to 19th century voting. I believe that the conditions have changed (especially given the electronic age with hidden cameras, hidden microphones, instant media communications, and so on) such that this type of fraud is no longer viable.

Here is text of a message to Peter Neumann, Kim Alexander, and David Jefferson--experts testifying before the California State Assembly. I elaborate on this point:

http://www.go2zero.com/re_ca_hearings.html

> Vote buying was a very big problem in the US at the end of the 19th century,
> and it worked because there was a verifiable receipt of how you voted.
>
Nowadays, vote buying goes on for sure but it's more subtle. I don't think any large-scale scheme like you fear could work today.

If this were a major cause for concern, we'd see a lot of this now with absentee ballots. This would be a much cleaner and less risky way to complete such a transaction.

In fact, it (direct vote buying) is a risk with absentee ballots and there have been some problems in this regard. It doesn't seems to be a major problem, however.

Logically, I don't think the state of California can object to giving the voter the ballot copy on this basis (fear of vote buying) while, at the same time, they allow anyone to vote absentee for any reason at all. Furthermore, in my discussions with Chris Reynolds of the Secretary of State's office, it seems they do not make this objection. There are appropriate laws on the books to discourage this type of thing.

In other words, I see no evidence at all that giving the voter the ballot copy would lead to any increase in vote fraud. On the contrary, I think it would greatly improve voter confidence in the system and thus strengthen the system. In addition, while most experts will say it's bad (giving the ballot copy), many other people disagree for mainly the reasons I give here (and elsewhere).

> See Thayer, Who Shakes the Money Tree, for some
> hillarious anectodtes.
>

I'm sure they some are hilarious. Peter Neumann went on and on about Edgar Allen Poe died on election day having downed several bottles of whiskey each earned from the several ballots he cast.

> We are currently sifting through many, many ideas,
> and trying to set up a forum at which some of these ideas can be addressed.
>

Please include me. I think you'll find that my system is the best. What other system has these features (to name a few)?:

- no manipulation of the vote can be hidden
- the voter gets proof that his or her vote was counted
- the voter gets proof of how his or her vote was recorded

In my proposal, I list 14 main features and benefits. No other system can match this.

--Alan Dechert

BILL NUMBER: AB 56 INTRODUCED
BILL TEXT

INTRODUCED BY Assembly Member Hertzberg

DECEMBER 4, 2000

An act to add Section 19006 to the Elections Code, relating to elections, and making an appropriation therefor.

LEGISLATIVE COUNSEL'S DIGEST

AB 56, as introduced, Hertzberg. Elections: voting systems.

Existing law requires the Secretary of State to study and adopt regulations governing the use of voting machines, voting devices, and vote tabulating devices.

This bill would require the Department of Information Technology to award grants to counties for the purchase of updated voting systems. Under the bill, a county would be eligible for the grant if it meets certain requirements, including, that the county provides matching funds to purchase the updated voting system at a ratio of $1 of county funds for every $3 of state funds.

This bill would appropriate $300,000,000 from the General Fund to the Department of Information Technology for this purpose.

Vote: 2/3. Appropriation: yes. Fiscal committee: yes. State-mandated local program: no.

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1. Section 19006 is added to the Elections Code, to read:

19006. (a) The Department of Information Technology shall award grants to counties for the purchase of updated voting systems.

(b) A county shall be eligible for a grant if the county meets all of the following requirements:

(1) The county has purchased, or intends to purchase, an updated voting system on or after January 1, 2000.

(2) The updated voting system is certified by the Secretary of State as utilizing the most current voting technology available at the time the county submits the grant request.

(3) The county provides matching funds to purchase the updated voting system at a ratio of one dollar ($1) of county funds for every three dollars ($3) of state funds.

SEC. 2. The sum of three hundred million dollars ($300,000,000) is hereby appropriated from the General Fund to the Department of Information Technology for the purposes of Section 19006 of the Elections Code.

ALAN DECHERT

4700 Allegretto Way, Granite Bay, CA 95746
voice (916)791-0456, adechert@aol.com

OBJECTIVE

Project management

SUMMARY OF QUALIFICATIONS

Fifteen years experience with computers: life-cycle application development, programming, user support, testing, hardware/software trouble-shooting and upgrading, network administration, e-mail, internet, software and hardware evaluation

Experienced as sales engineer for solar hot water, photovoltaics, and cogeneration

Quality assurance testing for DOS, Windows, Windows 95/NT commercial software

Professional writing and editing skills: newsletter articles, letters, advertisements, brochures, proposals, training materials, reports, evaluations, analytical papers, test plans

Experienced at giving presentations, lectures, training

Expert with dBASE, FoxPro, SQA Teamtest, MS Test, Visual Basic, and many other DOS and Windows PC software applications. Experience with HTML, Banyan Vines, Novell, Unix.

International testing. Enabling and localization. French, Italian, German, Spanish and some Japanese

EDUCATION

B.A. UC Berkeley — Music, 1978. Course work included 63 units in math, science, and computers. Company sponsored training in Banyan, Progress, Xponent, SQA Teamtest, *Testing Computer Software*

WORK EXPERIENCE

7/97 TO PRESENT:

Linda Rodgers and Associates, Senior Programmer Analyst
Consultant to Public Works Agency, Sacramento County CA.

- Developed application in Visual dBASE 7.5 to track drawings and equipment at the Sacramento Region Water Treatment Plant
- Upgrade, repair, enhancement of Visual Basic v6/Access application to manage County leases

- Year 2000 analysis and conversions
- *Application documentation.* Update existing application documentation
- Application maintenance. Feature additions and bug fixing.
- Office Automation process analysis
- *Address format standardization team.* worked with other county agencies (such as utility billing, police, 911, fire, county engineer, tax assessor) on defining a standard address table structure for all properties in the county. Also helped to define requirements for applications to use a central repository of addresses.

11/96 TO 3/97:

QA Engineer, Intel Corporation, Hillsboro, Oregon, testing Intel Internet applications. Contract position.

- Video Phone (POTS) testing on OEM platforms
- *Test documentation.* Test plan, test specification, test cases detail, for Intel Internet Video Phone
- Manual and automated test development and execution
- Bug reporting and tracking
- Testing, test planning for Intel Software Update Manager (ISUM). Made significant contributions toward improving the conceptual design of this product

2/96 TO 7/96

QA Engineer, Intel Corporation, Hillsboro, Oregon, testing Intel 28.8 DSVD modem. Contract position.

- Manual testing of remote control applications (Radish) for compatibility
- Automated testing using TAS telephone network emulation equipment
- Interoperability testing, manual and automated, with other v.34, v.32, and v.32bis modems
- *Data Analysis and presentation.* Developed an application to create summary reports from log files produced by test equipment. Developed a variety of reports for various internal and external clients

8/95 TO 2/96

QA Engineer, Intel Corporation, Hillsboro Oregon. Developed test scripts for

automated testing of internet applications (Browsers, FTP, email) for use with the Intel ISDN client software. Contract position.

- Debugged, ran, and analyzed results obtained with these test scripts and test scripts developed by other team members
- Manual testing for usability and compatibility
- Reported bugs and tracked bug history, updating and clarifying where necessary
- Installed and ran ISDN client software using foreign language (French, Italian, German, Spanish, Japanese) DOS/Win31 and Win95. Modified several test scripts to run under these languages

3/94 TO 1/95

QA Engineer, Borland International, Scotts Valley, CA. Began as contractor, later hired as regular employee. Tested dBASE DOS 5.0 and dBASE for Windows 5.0. Did some work on dBASE 5.5 for Windows (Visual dBASE)

- Tested the functionality and translatability of the U.S. product followed by testing of the translated versions.
- Used MS TEST for automated testing of dBASE for Windows
- Wrote test scripts covering all the new elements of the dBASE DOS language
- Revised the test shell for the largest of the automated test suites. This reduced the machine- hours required for these tests by 70%--with identical functionality.

2/93 TO 3/94

Consultant. PC Database applications and network installations

- Upgrade, modify and enhance Foxbase/Foxpro cost application for Morrison Knudsen/Parsons Brinkerhoff joint venture (Light Rail design project for the County of Santa Clara).
- Bibliographic database for California Environmental Protection Agency using dBASE IV

3/90 TO 1/93

Microcomputer Support Analyst. Morrison Knudsen Corporation, San Francisco, California. Transportation and Water Resources Division.

- Instrumental in successful implementation of Banyan network for this site. Experienced at installing server and client software, trouble-shooting server

and client problems (hardware and software). Developed and documented procedures.

- User support for WordPerfect, Lotus, dBASE, Foxpro, etc. for more than 200 users.
- Upgrade and repair of 'orphan' applications such as Man-hour forecasting application in DataEase. FoxPro, Foxbase, dBASE III, and dBASE IV application maintenance
- Developed, organized, implemented user training. Classroom and individual training.
- *Systems analysis.* Analyzed Office Services functions such as records management and purchase order system. Made appropriate recommendations; developed and implemented computerization resulting in more efficient operations.
- *Billable projects.* Using Foxpro v 2.0, developed bibliographic database system of scientific articles for Itaipu (world's largest hydro power installation) engineering staff.
- Project Performance Summary. Developed a one-page summary progress report for each of the large engineering projects. These reports were for executive use to give a thumb nail view of the status of multi-million dollar projects. I largely automated the process of compiling accounting and forecasting data from a variety of sources (IBM mainframe, WANG VS 100, project managers' PCs)
- Assisted Vice President in merging accounting data from a newly acquired company (Centennial Engineering). Developed programs for taking text reports from DEC VAX and translating chart of accounts into company standard.
- Developed an equipment management system in dBASE IV to track inventory of PCs and peripherals. Created other in-house dBASE IV applications such as an electronic Rolodex application for executive contact management.
- Evaluated hardware and software and made purchasing recommendations

11/88 TO 3/90

Independent consultant. IBM PCs & compatibles. Database applications development for business, government, and politics.

- Developed dBASE training for business users
- Developed dBASE IV application as sub-contractor for Spectrum Economics of San Francisco. This application tracks participation in the GAIN

(employment program) in Stanislaus County. Automated compilation of reports, statistics, etc. Trained users

- Developed database (dBASE IV) to process the results of several Spectrum Economics surveys and wrote numerous programs to produce statistical reports based on the data.

1/88 TO 11/88

Political Operative for the Democrats, 1988 election.

- Office Manager for the No. County Headquarters of the Santa Clara County Democratic Party.
- Responsible for coordinating the work of 8 paid staff persons and early 2,000 volunteers.
- Procured and maintained computer systems.
- Registration Coordinator for Santa Clara County Democratic Party. Organized successful registration drive resulting in over 25,000 new registrants. Developed program from scratch; recruited and trained volunteers, acquired and set-up computer systems; developed dBASE system for supporter tracking and to track progress and results of registration drive.
- Volunteer Coordinator for Jim Garrison for Congress. Recruited and trained volunteers for door-to-door canvassing effort. Responsible for campaign newsletter, the *Garrison Express.* Helped set-up computer system (dBASE III+, WordStar). Organized successful petition drive securing over 3,000 signatures to place candidate on ballot in lieu of filing fee.

1/86 TO 1/88

Sales Engineer G&G Solar of California, marketing solar energy and energy conservation products to commercial users. Cogeneration (small-scale packaged systems, e.g., TECOGEN 60kW).

- Feasibility studies, conceptual design, project development.
- Solar water heating systems for apartment buildings and commercial properties

10/82 TO 12/85

Sales/Sales Manager/Project Manager for Daystar Energy Systems of Alameda, California. Started as Sales Rep, became Manager of solar department within one year.

- Developed successful marketing program dramatically increasing sales and profits for the company

- Personal sales exceeded $800,000 in 1984
- Computerized operations; acquired and set-up computer system for the company (CP/M, dBASE II, WordStar).
- Bid, sold, managed installation of projects up to $300,000

1978 TO 1982

Piano Teacher. Maintained private teaching practice — in home studio.

PUBLICATIONS

Dr. Olov Östberg and Alan Dechert; "New Year's Eve 1999 -- What A Wonderful Night" *Öpnna System*; pg 4 - 6; October 1997 (Sweden)

Gary H. Anthes, "Worth all the fuss?"; *Computerworld*; pg 70; Nov 3, 1997

Elisa Williams, "The bills come in for the Y2K Bug"; *Chicago Tribune* Business.Technology section; pg 3; May 4, 1998

REFERENCES

References and further data furnished upon request

ASSOCIATIONS

American Society for Quality Control (ASQC)

Y2k

http://www.escribe.com/history/2000ad/m1809.html

T2k: Y2K and "Disappointment"

From: Richard Landes (view other messages by this author)
Date: Tue, 4 Jan 2000 13:07:55

Keywords: usenet, millennium

At 10:35 AM 1/4/00 -0700, you wrote:
>At 05:24 PM 1/3/00 -0700, JG wrote:
>--cut--
>>Keep your eye out for both apocalyptic and conspiracist spins on Y2K.
>Both are sprouting as we speak, as are those who defend the Y2K
musketeers
>as "miraculous heroes" and evoke an info-age auto de fe on heretics.

cognitive dissonance the morning after

some good stuff. chris lydon called me up on monday and on his show asked me "how is chicken little?" it's a little like being asked when i stopped beating my wife, trying to remind him that i had been careful to avoid becoming a c.l. is a lost cause from the start.

i must admit tho, and this list seems the like best to do it on, that i was wrong about y2k, and alan dechert was right, and all the more power to him because he could have used y2k to strengthen his argument for his Back2Zero calendar and didn't because there was no substance to it. if i write the "five books of histories" of this millennial cusp, i'll use your chronology, alan.

i think it is impt for y2k mavens who thought it wd be big stuff to think hard about why we found that scenario so compelling.

[.....]

CPSR Newsletter Winter 1999, Vol 17, No. 1

http://www.cpsr.org/publications/newsletters/issues/1999/Winter1999/neumann.html

[second half of article]

Unfortunately, there are no easy answers. Many different operating systems, application programs, programming languages, and databases are involved. Even if everything appears to work locally, interdependencies are likely to emerge when Y2K happens that could not be detected by testing. One of the largely unnoticed problems is that database management systems may have lurking two-digit data fields; heterogeneous combinations of database management systems may result in insidious incompatibilities if different fixes are used.

Intriguing risks can also arise from letting supposedly trustworthy third-parties fix your software. These risks include further flaws, theft of proprietary code, Trojan horses, and liability issues when the third party goes out of business on January 1, 2000. Note that many Y2K repair efforts for domestic software are being performed in other countries. This risk, of course, applies to other nations as well, some of which are in much worse shape than the United States.

One serious concern is that even if no Y2K technological problems occur when January 2000 rolls around (and I seriously doubt that we will escape unscathed), panic may set in as the end of the year approaches. The current Federal Reserve cash amounts would not be adequate if everyone decided to have more than (on average) $1,000 in hand for Y2K. Food hoarding is also likely. Moreover, there already appears to be a huge new market for electrical generators and emergency food rations.

To stave off panic, we may hear from government and utility officials that everything is under control, don't worry about a thing, everyone will be taken care of. But that is also not credible, especially in light of Stephen Horn's report card and the fact that many organizations have yet to begin assessing their vulnerabilities. Such reassurance also runs counter to the grain of logic, based on the archives of the Risks Forum, not to mention Murphy's Law. Even worse, Y2K represents an extraordinary target for terrorists, who just might have read the report of the President's Commission on Critical Infrastructure Protection (http://www.pccip.gov). Therefore, realism is required, as well as much deeper study of what the real vulnerabilities and risks are, and what must be done to reduce those risks. But throughout, we must not lose sight of the longer-range issues: there are many risks to the public in the use of computers and communications (for example, see ftp://ftp.csl.sri.com/pub/users/neumann/illustrative.ps or .pdf), and Y2K is just the tip of a very large iceberg.

Peter Neumann is Principal Scientist, Computer Science Lab; Chairman of the ACM Committee on Computers and Public Policy; Moderator of the Risks Forum; and member of the General Accounting Office Executive Council on Information Management and Technology (focusing largely on Y2K, particularly regarding the U.S. Government). He received CPSR's Norbert Wiener Award in 1997. His book Computer-Related Risks (Addison-Wesley 1995, more recent information on line) documents many of the risks involved in the use of information systems. You can reach him by email at Neumann@CSL.sri.com, or on the Web at http://www.csl.sri.com/~neumann/.

Dialog with Neumann

12/27/00
You wrote,

> Multiple use systems are always riskful for elections,
> because the accessibility to the other uses can result
> in compromises -- including operating system manipulations.
> ...

Several points:

1) The fixed disk is wiped; then an disk image (with OS and vote application) is copied on to it. So, you get a clean start. I know this is a bit tricky, especially with systems of various makes and configurations. But I know how to do it. We did it all day long at Intel (I used to be a test engineer there).

2) The setup person would follow some simple instructions to test the system and verify that it's working properly.

3) "Manipulations" cannot go undetected since the authentic vote is a piece of paper the voter reviews while in the voting booth. The electronic record of the ballot gets manually checked against the printouts by pollworkers before posting. Besides that, the voter can compare their own copy of the ballot with the public posting of the ballot on the Internet (only the voter knows the ballot number that belongs to them).

4) Using generic off-the-shelf equipment owned by various people and organizations in the community will help to de-mystify the equipment. While authorities may trust dedicated equipment (because they know the verification process) the public has no knowledge how this equipment has been tested and stored.

5) Dedicated equipment may carry significantly more risks. For example, suppose the touch screen equipment is used successfully for several elections and people become convinced that they are 100% accurate. So, after a while they are old and need maintenance. Verification may become lax over time presenting an opportunity for people maintaining the systems to install replacement parts that introduce bias. Procedures put in place to verify the equipment may not get followed--or there could be a conspiracy to rig the equipment. Dedicated equipment may depend on behind-the-scenes procedures for verification of individual votes and aggregate vote tally. The PC-Based Voter Certified Ballot is above board--the public can verify individual votes and aggregate tally. No "manipulation" can be hidden.

6) Even if the electronic record is totally destroyed or corrupt, it can be reconstructed from the paper ballots. The printouts (i.e., ballots) will be in a format that will be

especially easy for machine reading.

--Alan Dechert

Subj: Comments on Potential for Vote Buying in my Ballot System
Date: 1/20/01 8:53:51 AM Pacific Standard Time
From: Adechert
To: neumann@csl.sri.com (Peter G. Neumann)
To: kimalex@calvoter.org (Kim Alexander)
To: jefferson@pa.dec.com (David Jefferson)

Dear Peter, David, and Kim,

I enjoyed the comments you made during the California Assembly Committee hearings on Wednesday (Jan 17). It was nice to meet all of you, however briefly, and I hope you've had a chance to review the proposal I handed you. For your reference, this proposal can be found at:

http://www.go2zero.com/votereform.html

Mainly, I'm sending this email to counter one of the notions that you all have supported (and appears to be widely held by others): You say it would be wrong to give the voter a copy of their completed ballot. But before I get into that, I have some general comments about what I heard Wednesday.

Here are some of the best points made:

Kim noted that it is very important that the voters have confidence in the system. Assemblyman Longville raised an interesting question something like, "What if the system is secure and reliable but it is not perceived as such by the public?"

Peter said that a touch-screen system without a paper trail (like Sequoia) has no integrity since there is no proof that the code running at the time votes are recorded is the same code audited.

David pointed out that even if an electronic system is validated and becomes trustworthy, there may be problems down the road as systems are upgraded, repaired, or otherwise changed in circumstances that might not be so rigorously scrutinized as the years pass (this implies that it may be vulnerable to rigging at some point in the future).

I sensed two main fears amongst the legislators:

1) Fear that California might become another Florida.
2) Fear that California might become another California.

I think the hearing may soothe these fears somewhat but it's not clear how much was resolved. For example, the registrars seemed most interested in assuring everyone that they were doing a great job while saying things that clearly indicate gigantic holes in their assumptions, methods, and procedures. For example, at one point, one of the registrars (maybe Placer, I'm not sure) said that they "may" (if they have the time or something like that) return the request for an absentee ballot to the voter if the request is missing a signature in order to give the voter an opportunity to complete the request. I'm surprised no one jumped on that and I wanted to scream that that's exactly the type of thing that could make us "another Florida." Either you always return signature-deficient absentee ballot request for a signature or you never do. This lack of consistency opens the door to manipulation since whoever is making the decision on which ones to return could potentially favor one party or the other.

I could restate the second fear noted above as the fear that a major legislative remedy (widely regarded as a wise move at the time) to a problem could turn out to be a monumental disaster some years later (e.g., electric power deregulation). The fear may turn out to benefit the cause of ballot reform since it may make it less likely to plunge into something stupid.

Now to the heart of my message: I think it is widely felt that you can't give the voter a copy of their completed ballot. Your comments reflect commonly held views.

Paraphrasing,

Peter said, "you can't let the voter take it or else he'll be selling it for a bottle of whiskey."

Kim said "you can't give it to them because it opens the door to vote selling and vote swapping."

When I handed my proposal to David and explained that, "I give the voter the ballot." He responded, "Why would you do that? That would instantly lead to vote-selling."

I don't believe this assumption is correct. Clearly, I have a vested interest in showing that it's okay to give the ballot copy to the voter since my proposal amounts to nothing if this fact cannot be demonstrated. Allowing the voter to take a copy of the ballot is an essential feature of my proposal. The main advantage of my system over all others is that NO MANIPULATION OF THE VOTE CAN BE HIDDEN. If we cannot give the voter the copy, my system cannot work. So, I'm not exactly unbiased with this opinion. I feel quite certain I'm right, however.

Vote buying is not viable. Here, I need to make clear I'm talking about the blatant buying and selling you are suggesting. Someone says, "I'll give you x amount if you'll vote for me [or my candidate]. Bring me the printout to prove how you voted, I'll give you the money."

More subtle forms of vote buying go on all the time but this more blatant form cannot work and giving the voter the ballot copy would have nothing to do with vote buying. The basic reason is that in this post-Watergate era of sting operations, mass media, hidden cameras, hidden microphones, no solicitation for buying votes in this way could last for more than a few minutes before being broadcast on CNN or some other network. No campaign would undertake such a vote-buying program because the risk would be very high and the potential reward very small.

A common activity that's part of the Get Out The Vote (GOTV) effort on election day has to do with the campaign calling everyone in the precinct identified as a likely supporter in order to ensure that the voter gets to the polls. If the voter says, "gee, I don't think I can get there because I have a flat tire," (or whatever) the campaign figures a way to get the voter there. This is definitely a form of vote buying. The campaign spends resources on the voter in order to get a vote that would otherwise be lost. It's perfectly legal and it's done all the time. There are many other legal ways to buy votes.

Campaign consultants commonly talk about "cost per vote." The cost of one vote is typically in the 5 to 10 dollar range (can be even higher or even lower in unusual cases). So, depending on the brand and volume of the whiskey bottle, a campaign will generally do better to spend the money on legal methods rather than buying the voter a bottle of whiskey--even if they had reason to believe they could get away with it. But they could never get away with it.

If the system I am proposing were implemented and a campaign decided to try the vote-buying scheme you fear, imagine the process they'd go through. To whom will they make the offer and how will they do it? There is no point in offering to buy the votes of people already likely to vote for you. If they seek to buy-off voters likely to vote for an opponent, how long would it be before one of the voters loyal to an opponent would see this as an opportunity to ruin the vote-buying candidate? Not long, I submit.

Perhaps a poll would be in order:

Question: If a supporter of a candidate you oppose offered you $10 for your vote--payable when you submit proof of your vote--you would,

A. Cooperate with the person, vote accordingly, present the proof, and pick up the ten bucks.

B. Just say "no."

C. Expose the fraud.

Even if most people are dishonest (in their answer or their actions), this campaign clearly will not work. Some would certainly choose to expose the fraud. If the amount of money offered were substantially higher, you might get more people to cooperate but it would make no economic sense for the vote-buyer.

Swing voters might be targets for the vote-buyer. But an undecided voter is not necessarily one that could be swayed with an offer of $10. Some undecided voters will also have a high sense of morality just like voters that have already decided.

The likely target of the vote-buyer would be the apathetic, amoral bum. This fact presents many problems for the vote-buyer. This type of potential voter is not likely to be registered to vote. The vote-buyer would need to make deals with registered voters.

Paying for a vote in this way implies that a transaction must take place. The voter must supply the ballot copy to the buyer (for viewing or to keep) and then the buyer must hand over the cash. Most likely, this would need to happen in person (there are other possibilities such as mail or Internet but these methods entail other risks for buyer and seller). This sets up a very risky situation.

We can assume that in this situation the buyer and seller are both crooks by nature. So, the probability that one will try to cheat the other would be quite high. The buyer faces several problems. Two things right off:

1) The buyer could be blackmailed. The seller could document the transaction (hidden camera, for example) and then demand money to avoid exposing the fraud to the media.

3) The buyer could be cheated into buying forged ballot copies. How could the buyer authenticate the ballot copy? In my scheme, a reasonable looking forgery would not be very difficult. But a really good forgery would be nearly impossible. The ballot copy would contain some hidden information that would require key information held by election officials. Without the keys, the buyer could never really authenticate the copy.

To have any significant impact on an election, the vote-buying scheme would have to be known to many people. The odds of being discovered by the media and the authorities would increase dramatically with the number of people that learn about it.

Another possible target of the vote-buyer might be semi-literate, uneducated, and ignorant. This type of potential voter would not necessarily be inclined to do something illegal but might not understand all the implications. However, what chance is there that such a complicated transaction could be completed with significant numbers of these voters while maintaining the necessary secrecy?

So, this specific type of vote buying would be extremely risky for the buyer. Not only is it highly probable that such a scheme would be uncovered resulting in a felony conviction for the perpetrators and ruination of the candidate, but even if not exposed the buyer would face significant risk of blackmail and/or getting cheated into paying on fake ballot copies.

Vote buying goes on all the time. But only the more subtle forms are viable.

In short, I cannot fathom a circumstance where my system would lead to some new form of vote buying. If you can think of a circumstance where my system would lead to that, please describe it to me.

There are already laws on the books against the more blatant forms of vote buying. If my system were implemented, most any abuse could probably be prosecuted under existing laws. It's also possible that additional legislation would be needed to clarify some issues. In any case, I don't believe my system would suffer from law-breakers or any inability to control voting fraud.

The Issue of Trust

I think Kim was talking about one of the most important issues here: Do the voters trust the system? The experience in Florida reinforces the notion that "my vote doesn't count." It says that even if yours was the last vote counted and it was a tie before that, your vote still wouldn't count because the count would be so close that it would be recounted (maybe several times) and there would be a different result every time. So, the whole thing would likely be decided by the Powers That Be (a group to which you don't happen to belong).

We not only need to restore trust in the system, we need to go beyond that and instill a sense of trust that wasn't there before. Florida made things go from bad to worse. The widespread perception that "my vote doesn't count" was already there.

The Powers That Be tell the masses, "trust us to count your vote in a fair, accurate, and unbiased manner. You don't need to know all the details." Whatever new system gets adopted should not reinforce this edict. One of the dangers of electronic voting is that this edict will be further reinforced. At least now, we have some paper trail and some accountability. Electronic voting has the potential to concentrate audit responsibility into the hands of very few.

So, I feel that trust should be a two-way street. Voters need to be able to trust the system, but the elite cannot at the same time demonstrate absolute distrust of the ordinary voter.

My system has a nice balance. It expects voters to behave in a responsible manner but also has safeguards in case they don't.

--Alan Dechert

Subj: Re: Comments on Potential for Vote Buying in my Ballot System
Date: 1/21/01 12:46:28 PM Pacific Standard Time
From: Adechert
To: neumann@csl.sri.com (Peter G. Neumann)
CC: kimalex@calvoter.org (Kim Alexander)

CC: jefferson@pa.dec.com (David Jefferson)

In a message dated 1/20/01 11:32:19 AM Pacific Standard Time, neumann@csl.sri.com writes:

> Vote selling is as old as the hills.
>

This part is not in dispute. The question is whether or not giving the ballot copy to the voter would exacerbate the problem.

> Edgar Allan Poe died in the gutter as I recall
> (no, I was not there) in Baltimore on election day
> having voted several times and gotten several bottles
> of whiskey. ....
>

I see. Thanks for clarifying the "bottle of whiskey" reference in your comments before the CA State Legislature. I was wondering about that.

> But maybe it was not EAP and maybe it was
> not Baltimore and maybe it wasn't whiskey.
>

Maybe not. In any case, it might be tough to document--that is, the part about getting paid a bottle (or several bottles) of whiskey for each of his "several" ballots on election day. You might find documentary support for the Baltimore part and the whiskey part though.

In any case, the voting procedures and environment existing in the America of 1849 are not much relevant to ballot reform issues in the electronic age.

> Chicago, NY, and even Florida are notorious
> for vote buying and selling.
>

> Drunks who would otherwise vote are a fine target, because they
> might not even remember the next day and certainly would not be in
> a position to try to blackmail anyone.
>

"Drunks who would otherwise vote...."? Where would a campaign locate such people?

Seriously, a campaign targeting drunks ("that might not even remember the next day")? I don't see much potential there, especially since such people are not likely to be registered to vote. A campaign (in CA) would need to recruit such people about a month in advance

to get them registered. Then they'd have to find them on election day and take them to the polls. This doesn't sound cost-effective even if a campaign figured they could get away with it (which they obviously could not since they would be found out in the drunk-recruiting process).

Or maybe you are suggesting that the entire recruitment-payment procedure would take place on election day. How would this work? Let me guess. The campaign would set up some distance from the polling place and move in when they see a drunk staggering toward the door. "Hey, how about a bottle of this [opening cape]?" After the drunk staggers about (with his proof) the trasaction is completed.

> lack of a paper record of how votes were actually cast does not diminish
> the credibility of the process, because it provides no real assurance that
> votes were cast correctly, and indeed provides new opportunities for fraud.
>

Subj: Re: Comments on Potential for Vote Buying in my Ballot System
Date: 1/22/01 11:39:48 AM Pacific Standard Time
From: Adechert
To: neumann@csl.sri.com (Peter G. Neumann)
CC: kimalex@calvoter.org (Kim Alexander)
CC: jefferson@pa.dec.com (David Jefferson)

In a message dated 1/22/01 8:51:46 AM Pacific Standard Time, neumann@csl.sri.com writes:

> Sorry. Drunks who would otherwise NOT vote.
>
okay

> Actually, the Poe case is very well documented.
> I just don't have the references at hand.
>
I'll take your word for it. If it had happened within the past couple of decades, the details might be relevant. As it stands, with all the changes since 1849 in election laws, voter registration systems, ballot systems, campaign strategies, media coverage, etc., I wonder if these details have much bearing on the topic under discussion.

Seriously, you have asserted that giving the voter the ballot copy would lead to the most extreme form of vote buying ("I'll give you x amount to vote for my candidate. Bring me the proof of how you voted and I'll pay you."). You say that "Drunks who would otherwise NOT vote" would be good targets. But how would this actually worlk?

To examine this a bit further, imagine you are on the staff of a campaign organization and

that you are in a room where decisions are being made regarding how to apply the resources of the campaign to various vote-winning strategies.

Here are some of the likely topics:

Paid Advertising
- radio
- TV
- print media
- billboards
- direct mailings

Free advertising
- Identify individual journalists and how each might be dealt with
- How to get photo-opportunities in print and TV

How to convey the desired image of the campaign through these various media

Identify and discuss your opponent's strengths and weaknesses

Fund-raising events
- Identify times, places, and potential hosts

Overall campaign budget - identify sources and amounts of money raised and to be raised. Talk about how that money is to be spent.

How many votes are needed and where will they come from?

What are the polls saying? Are we where we need to be at this point in time and where do we need to be at future points in time?

Grassroots activities - door-to-door canvassing in the precincts ("precinct walking")
- precinct lists - how to obtain the best ones and how to use them
- what the canvassers should say and what literature should they hand out

In all of this, bear in mind that the campaign faces strict limitations on resources (money and people--paid staff and volunteers) and have only so much time to devote to any of these campaign activities. While each activity may or may not be discussed in terms of "cost per vote," it is understood by everyone that "cost per vote" is one of the overriding factors determining how the campaign allocates its resources.

Now suppose that a ballot system will be used where the voter leaves the polls with a copy of the ballot and someone on the team wants to explore how to take advantage of this. So, someone stands up to give a presentation on buying votes from "Drunks who would otherwise NOT vote."

Here are some topics to be covered in this presentation:

How to identify "Drunks who would otherwise NOT vote."
- canvass back alleys, flop houses, under bridges

How much to pay to each drunk

Timetable for main tasks
- identify target(s) (couple months before election day)
- negitiate agreement (verbal, most likely) with target
- get them registered to vote (about a month before election day)
- find them on election day
- transport them to the polling place
- arrange to pay them discreetly

Estimate total number of targets
- of those, what percentage will we be able to reach an agreement with?
- of those we make an agreement with, what percentage will we actually be able to find on election day?
- of those we are able to find on election day, how many will we actually be able to transport to the polling place (for example, if they are found passed-out somewhere, will we have sufficient manpower to lift them up and get them into the vehicle?
- of those we are able to find and transport, what percentage will be able to follow all the steps necessary to vote?
- of those we are able to find, transport, and are sufficiently competent to vote, what percentage will be able to live up to their agreement (some will forget, or change their minds, or sober up)?

What people will do this work?
- volunteers--how many do we have willing to do this work?
- paid staff--how many can we devote to this task?

Potential Risks
- felony convictions for those involved
- runination of campaign
- black mail

In order to minimize these risks, we must ensure two things:
1) Drunks must be sufficiently docile and forgetful that they will cooperate but will not be likely to remember any of it
2) Everyone in our campaign engaged in this activity must keep this a secret. Remember that "volunteers" routinely sign up for an opponent's campaign and act as double agents.

How likely is it that any campaign would buy-in to this plan? Apart from any moral,

ethical, and legal problems, it is clear that the cost per vote would be much higher (probably several times higher) than any of the usual methods of winning votes. This fact alone makes this plan not vialble. Even if a campaign thought it was viable and had the money to carry this out on a large enough scale that it could produce a significant number of votes, it would be impossible to keep it a secret. The campaign could scarcely approach more than a few hundred drunks with the proposition before the word of it would spread all over town. No campaign would ever adopt such a plan. It's preposterous.

Perhaps, Peter, you think a presentation (for buying votes from "Drunks who would otherwise NOT vote") could be made that some campaign would buy? I'd like to hear it. Please make sure you cover these topics since no campaign would undertake such a program without some idea of these factors.

How to identify "Drunks who would otherwise NOT vote."
How much to pay to each drunk
Timetable for main tasks
Estimate total number of targets and number of net votes gained
What people will do this work?
Potential Risks

You cannot put together a plausible sales presentation for this nor could anyone else. Any plan for a campaign to buy votes from "Drunks who would otherwise NOT vote" is just plain ridiculous. There may have existed conditions in 1849 that would make that work but those conditions do not exist today.

--Alan Dechert

Subj: Re: Comments on Potential for Vote Buying in my Ballot System
Date: 1/22/01 1:43:16 PM Pacific Standard Time
From: Adechert
To: neumann@csl.sri.com (Peter G. Neumann)
CC: kimalex@calvoter.org (Kim Alexander)
CC: jefferson@pa.dec.com (David Jefferson)

In a message dated 1/22/01 11:58:38 AM Pacific Standard Time, neumann@csl.sri.com writes:

> All of this discussion seemed academic before Florida,
> although there have been many close local elections that
> were resolved locally. I think we are focusing too narrowly
> on just one aspect of a huge system problem if we worry overly
> about vote selling.
>

I agree. Not only that, if a campaign had the resources and were really determined to buy

votes (and required proof before payment), they could hand the voter a little pocket scanner to be used on the ballot in the voting booth, which would then be returned to the campaign worker for payment. Giving the voter the ballot copy (as in my proposal) adds nothing to the potential for vote buying.

> ... However, a paper record that you can carry
> home as to how you voted adds almost nothing to the integrity of
> the big system problem, so it does not seem to me to be worth discussing.
>

I don't get it. It seems to me "most experts agree" that giving the voter the chance to see the actual completed paper ballot is an important check against an electronic ballot that might otherwise be subject to manipulation. I seem to recall that you talked about this last Wednesday at the hearing and said that you had recommended a system where the voter would be able to look at the ballot under glass before it would go into the ballot box. (a side note: you said this glass would have properties that would make it impossible to photograph--something someone else said couldn't be done. Anyway, this is an unnecessary precaution since anyone can carry a tiny hand scanner into a voting booth and make a copy of their ballot if they want. This has never been a significant problem--your impossible-to-photograph glass is a non-solution to a non-problem).

In my system, the take-home ballot copy adds to the system integrity:

1) The vote is published on the Internet so the voter can verify that their ballot was counted and counted correctly. No manipulation of the vote can be hidden. No other system I know of has such a safeguard. In fact, with most existing or proposed systems, the voter has no way to verify if their vote was even counted--let alone counted correctly.

2) While it may be possible to devise other voting systems that are perfectly reliable, my system gives the voter the chance to verify the vote. If a system were perfectly reliable and accurate but the means by which this was achieved was not comprehensible to the voter, it might add nothing to voter confidence in the system. I feel this is an important issue discussed some by Kim and Assembly Member Longville--I would like to have heard more on this subject. Lack of confidence in the voting system is very bad and simply reinforces the feeling (already fairly pervasive) that the rich and powerful control everything and the masses are just there to be manipulated. My system would add to voter confidence. This would probably be even more valuable than accuracy.

--Alan Dechert

Subj: Re: Comments on Potential for Vote Buying in my Ballot System
Date: 1/23/01 8:03:36 AM Pacific Standard Time
From: Adechert
To: neumann@csl.sri.com (Peter G. Neumann)
CC: kimalex@calvoter.org (Kim Alexander)
CC: jefferson@pa.dec.com (David Jefferson)

In a message dated 1/22/01 5:23:59 PM Pacific Standard Time, neumann@csl.sri.com writes:

> You may have noted Ed Gerck saying that their Internet Voting scheme
> allows you to verify that your vote was cast correctly. This provides
> no assurance whatsoever, because a shadow system could verify that
> your vote was indeed counted as cast, whereas the counting system could
> do whatever it likes.
>

I didn't catch all the details of this scheme so I'll take your word for it. However, my system does not have this problem. My system provides verification of the counting system as well. I thought I explained this pretty clearly in my proposal but maybe not.

The votes are posted (on the County Internet web server) for each precinct. The file is a simple ASCII text file (one vote per row) that can be loaded into any PC database or spreadsheet program. Verifying the count for one's own precinct is a no-brainer. The county would also have a page showing the totals for each precinct. This would be a bit more complicated spreadsheet due to all the different voting districts but would still not be difficult for your average spreadsheet jockey to verify the counts.

In my system,

* No manipulation of the individual vote can be hidden
* No manipulation of the count can be hidden

> NO ASSURANCE is BAD.
>
I agree. That's why I provide a way for the voter to verify the individual vote and also the count.

--Alan Dechert

Subj: Re: Comments on Potential for Vote Buying in my Ballot System
Date: 1/23/01 10:49:12 AM Pacific Standard Time
From: Adechert
To: neumann@csl.sri.com (Peter G. Neumann)
CC: kimalex@calvoter.org (Kim Alexander)
CC: jefferson@pa.dec.com (David Jefferson)

In a message dated 1/22/01 5:22:26 PM Pacific Standard Time, neumann@csl.sri.com writes:

> No problem letting them see it.
> Why do they have to carry it home?

>

In order to verify that it was counted correctly.

If you only let them see it, they can verify that what's on the ballot is what they intended, but they have no way of knowing what happened to the ballot after that.

In my system, they can track it down on the Internet by finding the ballot number. Every ballot has a unique id (key is actually state+county+precinct+ballot-number).

I thought about giving the voter only the precinct and ballot number on the second printout. This would eliminate some problems but would create others. A problem that would be eliminated: Say you accidently leave your ballot copy face up on the front seat of your car while you go to pick up Uncle Fester who happens to be a rabid NRA member. Uncle Fester notices that you voted against one of his favorite propositions that would have helped the cause of the NRA....

But here's a problem it would create: Say there's a proposition (Proposition 87T) that would prohibit construction of a 700 ft tall church on the corner of Elm and 43rd (a residential neighborhood). There were a lot of ads, billboards, and such about this. One billboard said:

NO 700FT TALL CHURCHES IN OUR NEIGHBORHOOD!

Yes on 87T

On election night, a voter notices that 87T failed and the church has the go-ahead to build. Enraged, the voter (with only the ballot number--no detailed printout) checks his vote on the Internet. He could swear he voted against the church and that everyone he knew was also against it. He sees that he voted "No" on 87T. He can't believe he could have made such a mistake. Surely, he must have voted "Yes" because he was against building the church. So, he claims that someone must have changed his vote.

Theoretically, at this point, the original ballot could be found and his challenge disproved. However, he might also claim that his vote was changed electronically and then the ballot was reprinted.

Additional safeguards might be taken to authenticate a ballot. For example, on election day all the paper that will be used could be stained with some special ink (say on the edge of the paper). After the polls close, all remaining paper stock is destroyed. So, any forged ballot could be found to be lacking this particular characteristic. However, if the voter is so certain that he could never have made this mistake he may claim the system must have been rigged regardless of any proof of authenticity of his original ballot.

Just providing the ballot number might not be good enough. If he had the actual detailed ballot copy, he could look at it and say, "I see... I voted No on 87T.... I blew it!" If he

lost or destroyed the ballot copy, he wouldn't be able to make the verification, but the rigging charge would make even less sense.

So, I say give 'em the ballot copy. They can choose not to keep it. In fact, I'd probably recommend that the polling place also have a shredder handy so that the voter can shred the copy before leaving if they are afraid of what might happen to the copy. Statistically, if only a small percentage of voters keep the copy and verify it against the published vote it will provide a good integrity check.

Moreover, if the voter has the copy and can verify that it matches the published vote, the voter will have much more confidence in the system. I believe that public confidence in the system is even more important than accuracy.

--Alan Dechert

Subj: Re: Comments on Potential for Vote Buying in my Ballot System
Date: 1/24/01 11:21:27 AM Pacific Standard Time
From: Adechert
To: neumann@csl.sri.com (Peter G. Neumann)
CC: kimalex@calvoter.org (Kim Alexander)
CC: jefferson@pa.dec.com (David Jefferson)

In a message dated 1/23/01 5:23:24 PM Pacific Standard Time, neumann@csl.sri.com writes:

> In Rebecca's scheme, the paper goes into a locked drum.
> Ideally, no one would ever look at it unless the exit polls
> differ wildly from the tallies -- as occurred in Florida.
>
Last things first: I'm not sure that any official procedures should depend on exit polls. Are you sure that's what you mean? As I recall, the Florida recount was triggered by the fact that the first count of the votes showed a margin of less than 1/2 of one percent. I don't think it had anything to do with exit polls.

As for the locked drum... who has the keys?

Does the voter have any way to check his vote in case he

The integrity of the system should be obvious and comprehensible to the voter. A system that has perfect integrity so long as the technocrats follow procedures but where nothing can be verified by the individual voter, may not inspire much confidence.

The Florida situation was probably something like a once-in-a-hundred-years phenomenon.

Longville asked (paraphrasing), "What if a system has proven integrity but is not

perceived as such by the public? Will we be better off?

Just because top scientists and engineers say a system is "fail-safe," will not necessarily inspire great public confidence. As fine as Rebecca's scheme might be, it doesn't sound like the voter has any way to personally verify how their vote was finally counted nor verify aggregate totals.

I consider John Longville's question

Can we safely assume a public official of high rank would never do anything to throw an election? We can probably devise a system so that no individual would have that capability. But what about several people acting together? Can we assume that several high ranking public officials would never conspire to throw an election?

Subj: Re: Comments on Potential for Vote Buying in my Ballot System
Date: 1/25/01 10:25:17 AM Pacific Standard Time
From: Adechert
To: neumann@csl.sri.com (Peter G. Neumann)
CC: kimalex@calvoter.org (Kim Alexander)
CC: jefferson@pa.dec.com (David Jefferson)

In a message dated 1/24/01 12:17:53 PM Pacific Standard Time, neumann@csl.sri.com writes:

> If not for the exit polls in Florida showing the INTENT of the voters,
> the discrepancies might never have surfaced. The 14% dropoff for the
> Senate vote in 1988 in the same four Florida counties went almost
> unnoticed.
>

Didn't exit polsters say (around 6pm PST) Gore won Florida (which would have wrapped up the election for Gore)? A little while later, they gave it to Bush. Then they said, "whoa! too close to call." I mean, why vote? Why not just watch TV and let them tell you who won before you ever get to the polling place?

Thanks guys. This type of media manipulation (using exit polls) adds to the perception that "my vote doesn't count." That's BAD.

> Locked drum? TWO keys? Welded shut with a trusted path for stuff
> to enter? Lots of strategies. you can think of a few that YOU
> might be satisfied with, if you try.
>

I see one huge locked drum for the county. No, I see one locked drum for each precinct. Or, it could be one locked drum for each voting booth. It could be many keys. I don't know.

It seems to me that Rebecca's system--fine it may be--involves purchasing a lot of proprietary, dedicated, expensive hardware that will have to be stored and finally replaced over a period of years.

My system for sure involves more people power, but it doesn't require purchasing a lot of new hardware.

> The integrity of the system will NEVER be obvious and comprehensible
> to the voter. There are too many weak links.
>

Perhaps, strictly speaking. Maybe I should say it should seem relatively obvious and comprehensible to the voter. Voters may not understand much about the details of how there PCs work, but they have a high-level comprehension of them since PCs are so ubiquitous.

Perception counts for a lot. If people have no confidence in the system, they might think blowing up a building might be a better way than participating in the system.

> Florida has happened MANY times before, just not on a presidential
> scale where a few votes swung in one precinct could swing the entire
> election nationwide.
>

No. In this context, that's like saying "Ford was assassinated too, the bullets just didn't happen to hit him." "Florida" has never happened before. To refresh your memory, here are a few unique features of "Florida."

- The attention of the entire country (and a lot of other people around the world) largely focused (for more than a month) on issues like "butterfly ballots," "hanging chads," errors handling absentee ballot requests, recount procedures,

- We see how any of several decisions about election day procedures could have thrown the election one way or the other.

- US Supreme court ends it, saying in effect: "We don't know if your votes were counted right, but we sure know how are votes are counted! Losers!"

Nothing like this has ever happened. The "presidential scale" (which you prefer to wave aside with a flick of the wrist) is what made it unique and important.

I don't think it's necessarily a bad thing, what happened. It's an opportunity. We saw just how bad things are with our voting systems. Who knew? (I suppose you did, but the vast majority had no idea). Who knew those punch cards had such a high error rate? Who knew that a state legilature could lay out such vague criteria so as to

accommodate upteen different types of voting methods.

Now, a lot of people know these things. This event may also give us some clue of why so many people think "my vote doesn't count." Now, we have a real opportunity to improve the situation--build confidence in the system and engage more people in the process.

--Alan Dechert

Subj: Re: Ballot Reform Discussion
Date: 1/26/01 10:55:14 AM Pacific Standard Time
From: neumann@csl.sri.com (Peter G. Neumann)
To: Adechert@aol.com

I don't really have the time, but I think you have an interesting approach -- although it ignores problems that I think are important. On the other hand, I think we are likely to see some really inadequate systems emerging in the rush to do something different, especially in the light of the malicious insider problem.

References

Curtis Gans
Committee for the Study of the American Electorate
202-546-3221

Richard McCann, Ph.D
M.Cubed
2655 Portage Bay, Suite 3
Davis, CA 95616
(530) 757-6363/757-6303fax
rmccann@cal.net

Richard Landes
Boston University History Department
617-353-2558 (of)
617-353-2556 (fax)
http://www.mille.org/
rlandes@bu.edu

Sacramento County References

Josie Johnson, 875-6781
PWA MIS Bradshaw Team Lead

Debbie Nadolna, 875-6724
PWA MIS Chief

Ray Levitt, 875-6647
Utility Billing Supervisor

Brad Belletto
Principal Engineering Technician
SRWTP - Contract Documentation
875-9085

Carolyn Rice, 875-6627
Water Quality Supervisor

Forrest Horner, 875-6647
Business Analyst

[this is Alan Dechert's talk given at the UC Santa Cruz forum on electronic voting held OCT 26th 2003]

Good afternoon. I thank *all* of you for coming. *I* am *glad* to be here. Thanks also to Bob Kibrick and Arthur Keller for their work in organizing this forum. I also want to say thank you to all the others at UC Santa Cruz that helped make this possible, and to all the other forum speakers.

Ladies and Gentlemen, we have a problem. Our voting system is broken. It does not need to be repaired, however. *It needs to be replaced.* We don't need to upgrade our voting system. We need to replace it. We don't just need some new voting machines. We need a whole new idea for how to administer public elections.

This afternoon, I will describe the work some of us are doing to bring about a better system. But first, I want to take a few minutes to set the context.

Sovereignty is the right to decide. Sovereignty means *the right to decide.*

In a democracy, sovereignty is … *distributed.* In a democracy, sovereignty is distributed, while *you* — the individual citizen — retain most of this right to decide.

We share this right. We distribute sovereignty. The system for distributing sovereignty is called democracy. In a democracy, we distribute sovereignty through our system of laws. The

voting system is part of the system whereby we share our right to decide. Sometimes, we vote to decide on *specific issues*. But mostly we vote for *people* who will make decisions for us.

While democracies all share the rule-of-law concept, they vary widely on voting systems. In the U.S., it seems that we vote on *everything*. We vote for everything from President to dogcatcher. We vote on a lot of initiatives.

We tend to *consolidate* the administration of elections. While we're electing federal officials, we say, "Let's put state and local contests on the same ballot with them." This is *very* unusual. Only the Swiss do something similar. In most democracies, you vote for your Member of Parliament *and that's it,* at the national level. Local elections are separate and may be administered — as in Canada — with different rules and different equipment by different entities.

Is our system more democratic because we put more things on the ballot? Not necessarily. It is not practical to present every issue to the people for vote — no government even *attempts* to do that. The vast majority of political jobs are still appointed. Something like 2,000 jobs were at stake in the recent contest for Governor of California. Democracy is not proportional to the number of offices and issues on which the people vote.

Do we really need so many elected offices, anyway? An idea going back to ancient Greece suggests maybe not. Most officials were chosen

by *sortition:* They were chosen by lottery from a pool of qualified individuals.

Our voting system varies *within* the United States. Voting systems vary from state-to-state and county-to-county. Warren Slocum is the chief of elections for San Mateo County. He was *elected:* most of his counter- parts in other counties were *appointed.*

In January of 2001, I attended a hearing conducted by the State Assembly's Elections committee. Some of the testimony was incredible. One of the many horror stories had to do with a man that was not registered to vote where he lived on one Election Day, and was given a provisional ballot. For some reason, he seemed to like voting with the provisional ballot. So, rather than re-registering, year-after-year he voted a provisional ballot. Only one problem: his votes were *never counted.* We can only speculate why he didn't want to be in the normal voter file; but sometimes voter lists have been used for marketing, and they are also used to find people for jury duty. There are several reasons someone might like *not* to be on the list but still be able to vote. Anyway, after a few years, the elections people recognized his signature by sight but it was against their policy to inform owners of provisional ballots whether or not their vote was accepted. Year after year, his vote was *thrown out.* Now, how *dumb* is this system?

At least in Iowa, if you go to the polls to vote and you're not on the roster, they will give you a provisional ballot but they will also make sure you get registered to vote at the same time.

Voters should not be disenfranchised by the voting system. By voter disenfranchisement I am talking about cases where votes are not counted the way the voter intended, or the vote was not counted at all, or the voter was discouraged from voting altogether — even though registered to vote. Furthermore, I am talking about cases where potential voters were discouraged from registering to vote.

If we're going to have voter registration — and it's not clear to me that we need it — it should not be an obstacle for voters. But currently, it *is* an obstacle.

In Georgia, in order to vote you have register by the 4th Friday before Election Day. In Ohio, the deadline is 30 days. In Iowa, it's 10 days before any Primary or General election, but *11 days* for other elections. It's the 3rd Saturday before in Vermont, *but you only have until noon* to get your paperwork into the town clerk. In North Dakota, they do not have voter registration. In Idaho, the deadline is 25 days before Election Day but then you can register on Election Day itself. What if you moved from Idaho to California a week or two before Election Day? You might think you would still be able to register on Election Day. You would be *out of luck.* ***Rarely*** an issue, you say? Consider that almost one million Americans move in any given week. Over a million voters could be impacted by the logistics of moving while having *"register-to-vote"* on a long to-do list.

At a minimum, Election Day registration should

be universal. In the long run, we should investigate how we can *eliminate* voter registration altogether. Afterall, if you are a citizen of voting age and you meet all the requirements, you are also in many databases. Why have another database that has serious maintenance issues for the voters as well as state and county governments?

As I see it, voter registration, provisional ballots, and a whole lot of the other rigmarole and gobbledygook are artifacts of the 20th century — before the Internet and before the personal computer. In this new century, every polling place should be securely connected to the Internet. Studies have shown that while you will probably never be able to vote remotely over the Internet *unattended,* it should be possible to vote over the Internet at poll sites where your identity can be confirmed. We should look at this as a possible replacement for current absentee ballot methods.

In the wake of the election mess in 2000, the presidents of Caltech and MIT launched a project they hoped would bring about a solution to the voting system… conundrum. Their December 14th 2000 press release was titled, "Caltech and MIT Join Forces to Create Reliable, Uniform Voting System." Note the word, *"uniform."* In other words, they noticed — like most of us — *the great variety of faulty procedures.* Then they said, "Let's create *new voting technology,* test it thoroughly…make it bullet proof … then use the same equipment and procedures *everywhere."* Why not have a *uniform* system? Why have all

these *daffy different* ways of doing the same thing? Why not find one way that really works and use that?

Quoting the beginning of the press release,

> The presidents of MIT and Caltech have announced a collaborative project to develop an easy-to-use, reliable, affordable and secure United States voting machine that will prevent a recurrence of the problems that threatened the 2000 presidential election....

Okay, so they wanted to develop a U.S. voting machine. It sounds like they started with a really good idea. But now, almost three years later, *where's their voting machine?* Where is this technology they were talking about? This is not rocket science, folks. Maybe that's the problem. Caltech and MIT are good at rocket science. They know how to do that. But the obstacles here are mainly political. The voting system represents a significant technical challenge, but it's mainly applied science. Technically, this is not horribly difficult. Politically, *it is a **pain.***

Of course, *I* think they had the right idea. In fact, I published a similar idea about the same time as their announcement. Before you ask, "Okay, now, three years later, where's Alan Dechert's voting machine?", let me make this point: I am critical of Caltech and MIT researchers because they started with a lot of money and tremendous institutional support. They did not follow through with the idea. I started with none of these

resources. Maybe you will say, "He's just envious." And maybe that's it: I'm just envious of their resources. But the fact is that when it comes to the idea of a uniform system and a U.S. voting machine, I have moved the idea forward while they have not. I also incorporated the open source concept and the voter-verified printed ballot. Caltech/MIT never embraced these ideas. They abandoned the idea of a uniform system and chose to work with existing vendors in effort to improve voting systems.

There is still a Caltech/MIT voting project and they are doing some good work — uncovering information and helping to improve things here and there. But *it is not* the magnificent work they set out to accomplish.

I am developing the Open Voting Consortium as a durable organization to develop, transfer, and maintain this new voting technology. There is no need for expensive dedicated hardware: we can use inexpensive off-the-shelf commodity PCs and peripherals, while utilizing *free* software. Once our open voting system becomes established, the persistent issue of how to replace obsolete hardware will be gone forever. Usually, we're happy to pay a little more to get something better. It happens that our system will be *much better,* but also *much much cheaper.*

A secure, reliable, trustworthy, and affordable voting system is an essential feature of a successful democracy. A voter-verified paper ballot is an essential feature of a successful voting system.

To give you an idea of what *your ballot* may look like in the future, I've passed out some samples in folders like this [hold up sample]. With our system, you print the ballot yourself on ordinary eight-and-a-half by eleven paper in the voting booth, and then place it in a privacy folder like this. You'll notice about half an inch of the ballot is exposed. The exposed border has the barcode, but no other printing.

This part of our demonstration system — the ballot printing function — is done. It's on the Internet, and available for anyone try out.

This is what we mean by a voter-verified printed ballot. You go to the computer; make your selections; print it out with the touch of a button, and look to verify that these *are* the selections you intended to make. If not, you can destroy this one and start over. No problem. There are no hanging chads, no ambiguous marks. No voter intent issues — it's all written out very clearly.

What if because of some disability you can't read the ballot? First of all, you would have voted at a station where all the selections were presented orally through headphones, much like the way existing electronic systems work. *Unlike* existing systems, however, you would have an opportunity to actually *verify* how your vote was recorded. It is *not possible* to verify your vote on existing electronic voting machines — visually or otherwise. Anyone claiming voter verifiability for these paperless systems is telling fairy tales. At best, all you can get is some indication that the machine knows what selections you want to make. This may or may not have anything to do

with how your vote gets recorded. With our system, *even if you can't read it,* you will print the ballot just like everyone else. If you want to verify your ballot, you can go to a station with a scanner, and have the barcode scanned while you're wearing headphones so you can hear your selections read to you. The ballot does not have to be removed from the folder: Your privacy is assured. Then you go to the ballot box and deposit your ballot like everyone else.

Right now, we also have the software available for download that will take the encoded information from the barcode and read back the selections. If you want to try that out, it's available. We'll have a full demonstration of our system ready in a few weeks.

In summary, while technology has taken great strides forward in recent decades, the voting system has not kept up. The problem of modernizing the system has been routinely underestimated. It's *very* complicated.

The technical complexity is routinely underestimated, *but we know how to do it.* It is the *political* complexity that boggles the mind and tests our resolve. But our team is meeting this challenge!

THANK YOU.

Response to:

"American Attitudes about Electronic Voting" Survey
By Thad Hall and Michael Alvarez
http://www.vote.caltech.edu/Reports/fall04survey.pdf

And Advice for Utah's Voting Equipment Selection

TO:
University of Utah Behavioral & Social Science Department
Governor Olene Walker
Lt. Governor Gayle McKeachnie
Amy Naccarato, Utah State Election Office
Utah Procurement
Val Oveson, CIO of the State of Utah
New York Times re: "Electronic Voting Steps onto the National Stage" news (article Sept. 19)

FROM:
Erik Brunvand, Associate Professor of Computer Science, University of Utah
John Carter, Associate Professor of Computer Science, University of Utah
Alan Dechert, Open Voting Consortium, Founder and President
David L. Dill, Professor of Computer Science, Stanford University
Kathy Dopp, MS Mathematics, U of Utah, Utah Count Votes Founder
Ganesh C Gopalakrishnan, Professor of Computer Science, University of Utah
David Hanscom, Professor of Computer Science, University of Utah
Michael Jones, Assistant Professor of Computer Science, Brigham Young University
Arthur Lee, Associate Professor of Computer Science, University of Utah
Jay Lepreau, Research Professor of Computer Science, University of Utah
Kent Seamons, Assistant Professor of Computer Science, Brigham Young University
Peter Shirley, Associate Professor of Computer Science, University of Utah
Barbara Simons, IBM Research (ret), former president,
Association for Computing Machinery (ACM)
Pamela Smith, National Coordinator, Verified Voting Foundation
Phillip Windley, Associate Professor of Computer Science, Brigham Young University and
Former Chief Information Officer (CIO) of the State of Utah

Utah has the time to do the right thing and benefit from other states' collective experience and research. Expert computer scientists should help to create specific criteria for all aspects of our voting systems. Utah can join multi-state open source development efforts and write a more specific RFP next spring that details the State's real requirements, including a VVPB, and allow sufficient time for a thorough review, including outside experts, to ensure that Utah's voting system is the most secure and trustworthy in America.

We are writing this letter because we are concerned by the interpretations presented in the "American Attitudes about Electronic Voting" Survey, co-authored by Professors Thad Hall and Michael Alvarez. Furthermore, the interpretations in the study can do significant harm because the State of Utah is in the process of purchasing new voting machines, and this study could

have a major impact on that decision. "Would they ask questions about the safety of a medical procedure of patients or of doctors?" asked Professor Avi Rubin of Johns Hopkins in a recent Computerworld interview. "They should ask computer security experts about computer security questions, not end users, who may like the look and feel of the machines but have no way of knowing if they are really secure."

In this letter, we have detailed some of our concerns and made our suggestions. We would be delighted to discuss any of the specifics with you.

Our Response to "American Attitudes about Electronic Voting" Survey

We feel that it is critical that voters have the opportunity to vote and that their votes be accurately counted. A voter-verifiable paper ballot is necessary to ensure the integrity of our elections.

> *The American Attitudes Survey's executive summary states "If ... voters lack confidence in electronic voting systems ... the basic integrity of our democratic system could be in jeopardy."*

We concur. However, the integrity of voting systems is not determined solely by public perception. As much as we would like to believe that computerized systems are less prone to problems than their non-computerized counterparts, the Caltech-MIT Voting Technology project found that electronic voting machines' rates of unmarked, uncounted, or spoiled ballots are among the highest rates of any voting technology. Hand-counted paper ballots and optically scanned paper have the lowest error rates.

Key findings of the "American Attitudes about Electronic Voting" survey are not substantiated by its own data. For example:

> *The American Attitudes Survey's key finding #1 says "American registered voters are largely comfortable with the two predominant voting technologies: electronic and optical scan machines." In the NY Times "Electronic Voting Steps onto the National Stage" (news article Sept. 19), this finding is further repeated: "Despite Concerns, Americans Are Comfortable with Electronic Voting" above a chart labeled "Which of the following ways to cast your vote are you most comfortable with?"*

Unfortunately, the survey question upon which this statement and the chart are based is flawed. We believe that no such conclusions can be fairly drawn from the data.

The survey question asked by the American Attitudes Survey was:

> *"Regardless of whether or not you have voted in the past, which of the following ways to cast your vote are you most comfortable with? Electronically, like on new touchscreen machines, marking a paper ballot with a pen, by punchcards, or by some other method?"*

First, Optical scan machines were not explicitly mentioned in the survey question and since optical scan ballots can be created either electronically or by marking a paper ballot with a pen,

people who prefer optical scan systems might have selected "new touch screen machines", "marking a paper ballot with a pen", or "some other method". (E.g. Voters were not presented with an option that allowed for electronic optical scan technologies such as an electronic voting interface that generates an optically scan-able ballot or an optical scan vote that is scanned at the precinct level and reported electronically).

Second, no selection for "hand-counted paper ballots" was offered. Persons who prefer hand-counted paper ballots would most likely select "marking a paper ballot with a pen", the same category that the authors attribute to "optical scan" machines.

Further, this survey question asks about "casting" votes, *not* about counting votes. While a voter might be comfortable casting their vote (purely) electronically, many of us would be extremely uncomfortable having our votes counted and reported purely electronically. A voter's comfort voting with a particular technology does not imply that they are comfortable with their vote being counted with that same technology.

In addition, other survey data indicates that almost 40% more people agree than disagree with the statement that "Electronic voting systems increase the potential for fraud" AND almost twice as many agreed than disagreed with the statement that "Electronic voting systems are prone to unintentional failures."

In general, the raw data reported as part of the survey does *not* support the author's claim that "American registered voters are largely comfortable the two predominant voting technologies: electronic and optical scan machines."

> *In their introduction Professors Hall and Alvarez say "... there have been cases of electronic voting machines... lowering the number of uncounted ballots."*

While that is true, in 2000, electronic voting machines' rates of spoiled, uncounted, or unmarked ballots were only less than the rates of mechanical lever machines and the most error-prone type of punch card machines according to the MIT/Caltech Voting Technology Project. Utah punch card error rates have been lower than the national average due to intelligent election procedures involving thorough testing of ballot definitions, inspection and cleaning of ballots prior to counting, and routine cleaning and emptying of our punch card machines. Errors of (purely) electronic voting machines may often be undetectable and there are many instances of (purely) electronic voting systems reporting highly improbable outcomes, forcing the relevant voting officials to explain the seemingly impossible results with comments that boil down to "the computer says its true, so it must be."

Proponents of paperless electronic voting systems, such as Dr. Hall, cite the "chaos" of adding printing systems to voting equipment and call critics of purely electronic voting "political elites" who raise doomsday scenarios. Unfortunately, these scenarios are neither unlikely, nor do they require vast conspiracies. Problems as simple as a computer bug or configuration error by election workers can and have caused serious errors in recording votes. Over 2000 technologists have endorsed Verified Voting Foundation's resolution saying "Computerized voting equipment is inherently subject to programming error, equipment malfunction, and malicious tampering..."

The current generation of electronic voting machines are not secure, do not provide voters with a way to know that their votes are being tabulated correctly, and do not provide a mechanism for effective recounts when errors arise. As such, they represent an unacceptable technical risk, regardless of how people feel about them. The only way to effectively guard against errors is to have a redundant system for counting votes. The authors of this response strongly feel that the only technology currently available that provides this necessary redundancy is Voter Verifiable Paper Ballots (VVPB).

Recommendations to the State of Utah on Voting Equipment Selection

The State of Utah has roughly $20 million to spend on the research and development or purchase of new voting systems. The State's Voting Equipment Selection Committee recently issued a request for proposal (RFP) for voting equipment.

Fifteen Computer Science professors and voting experts sent a response to the Utah Voting Equipment Selection Committee citing significant problems with Utah's RFP. (See http://www.UtahCountVotes.org/response.pdf) The problem with the State's current RFP is that it contains almost no specific requirements about what the State needs. As written, the RFP is an invitation for vendors to tell the State what it needs. That is a poor way to do purchasing in general, but in the case of something as important as voting equipment, it is downright dangerous.

Utah's current RFP does not appear to allow sufficient time to conduct proper security reviews of the proposed systems. Further, Utah's RFP does not require electronic voting machines to issue a voter verifiable paper ballot (VVPB). A VVPB records the voter's intentions and allows the voter to verify that the ballot has correctly printed those intentions. The VVPB is then stored separate from the voting machine to allow an independent recount of the election results. An overwhelming majority (over 95%) of computer professionals who participated in a survey conducted by the Association for Computing Machinery (acm.org) agreed that electronic voting systems should "provide a physical record so voters can inspect permanent records of their ballots before they are cast and so meaningful recounts may be conducted"!

We applaud the voting equipment selection committee's efforts to improve Utah's voting system. We simply want the result to really be an improvement.

See pg 2

Appendix A

Contributors to the Commission's Work

The following individuals directly contributed their expertise to the work of this Commission. Forty-eight of these individuals testified at one of our four public hearings. Others participated in the work of the task forces. Still more offered written submissions to our work. We acknowledge them below.

The Commission wishes to express its gratitude to these experts, as well as to the hundreds of citizens from across the country who, in the democratic tradition, generously contributed their opinions for this report.

For those individuals who testified in a public session of the Commission, we have noted the date and place of their testimony so that interested researchers can locate the transcripts of what they said. All of the hearing transcripts are available at www.reformelections.org.

Congressman Roy Blunt (R-MO)
William Boone

Jim Adler
VoteHere.net

Kim Alexander
California Voter Foundation
Ronald Reagan Library, April 12, 2001

Howard Allen
Southern Illinois University

R. Michael Alvarez
California Institute of Technology
Ronald Reagan Library, April 12, 2001

John Anderson
Center for Voting and Democracy
written submission

Stephen Ansolabehere
Massachusetts Institute of Technology

Peter Argersinger
Southern Illinois University

Tim Augustine
Maryland State Board of Electors

Larry Bartels
Princeton University

Robert Bauer
Perkins Cole LLP

Chris Beem
Johnson Foundation

Robert Bell
Democrats Abroad Canada
written submission

William Boone
Clark Atlanta University
The Carter Center, March 26, 2001

Kimball Brace
Election Data Service, Inc.

Henry Brady
University of California, Berkeley

Bill Bradbury
Oregon Secretary of State
Ronald Reagan Library, April 12, 2001

Philip Breen
United States Department of Justice

Polli Brunelli
Federal Voting Assistance Program

Walter Burnham
University of Texas

Dianne Byrum
Michigan State Senator
written submission

David Capozzi
The United States Access Board

Jo-Anne Chasnow
Human SERVE Campaign

David Chaum
SureVote, Inc.

Henry Cuellar
Rodolfo de la Garza

Ryan Chew
Office of the County Clerk, Cook County, Illinois

Charlotte Cleary
Registrar, Arlington, Virginia

Jennifer Collins-Foley
Los Angeles County, Registrar-Recorder/County Clerk

Cathy Cox
Georgia Secretary of State
The Carter Center, March 26, 2001

Gary Cox
University of California, San Diego

Kristen Cox
National Federation of the Blind

Paul Crafts
Florida Department of State

Charles Crawford
American Council of the Blind

Henry Cuellar
Texas Secretary of State
LBJ Library, May 24, 2001

Alan Davidson
County Clerk, Marion County, Oregon

Donetta Davidson
Colorado Secretary of State

Michael Davidson
The Constitution Project

Rodolfo de la Garza
University of Texas
LBJ Library, May 24, 2001

Alan Dechert
University of California, Berkeley
written submission

Daniel DeFrancesco
New York City Board of Elections
written submission

Karen Delince
American Civil Liberties Union
written submission

Jim Dickson
American Association of People with Disabilities
Gerald R. Ford Library, June 5, 2001

Christopher Dodd
United States Senator for the State of Connecticut
Gerald R. Ford Library, June 5, 2001

Craig Donsanto
United States Department of Justice, Election Crimes Branch

John Dowlin
Elections Division, Hamilton County, Ohio

Jennie Drage
National Conference of State Legislatures

Maria Echaveste
Democratic National Committee
LBJ Library, May 24, 2001

David Elliott
Office of the Washington Secretary of State

Kathy Fairley
District of Colombia Board of Elections and Ethics

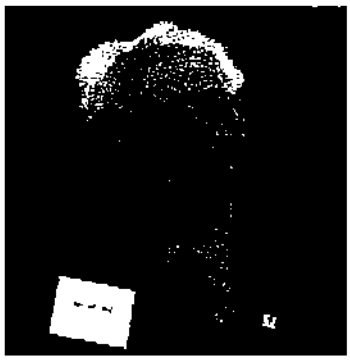
Margaret Fung
Asian-American Legal Defense and Education Fund

Curtis Gans
Committee for the Study of the American Electorate

James Gashel
National Federation for the Blind
LBJ Library, May 24, 2001

James Gimpel
University of Maryland

Rosalind Gold
National Association of Latino Elected and Appointed Officials (NALEO)
Ronald Reagan Library, April 12, 2001



J. Kenneth Huff, Jr.
Bob Irvin

Stephen Gold
Disabilities Law Project

Ralph Goldman
Center for Party Development
written submission

Lance Gough
Chicago Board of Election Commissioners

Gary Greenhalgh
Election Systems and Software
written submission

Michele Grgich
General Accounting Office

Kenneth Gross
Skadden Arps Slate Meagher & Flom LLP

Scott Harshbarger
Common Cause
LBJ Library, May 24, 2001

David Hart
Hart InterCivic

Ernest Hawkins
National Association of County Recorders and Clerks
Gerald R. Ford Library, June 5, 2001

Jeffrey Hayes
Market Strategies

Kris Heffron
City of Los Angeles Elections Division

Andrew Hernandez
Southwest Voter Registration Education Project

Hendrik Hertzberg
Center for Voting and Democracy
LBJ Library, May 24, 2001

Steny Hoyer
Member of the United States Congress for the Fifth District of Maryland
Gerald R. Ford Library, June 5, 2001

Zoe Hudson
The Constitution Project

J. Kenneth Huff, Sr.
AARP
LBJ Library, May 24, 2001

Asa Hutchinson
Member of the United States Congress for the Third District of Arkansas
The Carter Center, March 26, 2001

Bob Irvin
Georgia General Assembly
The Carter Center, March 26, 2001

Maxine Issacs
John F. Kennedy School of Government, Harvard University

John Jackson
University of Michigan

Gary Jacobson
University of California, San Diego

Alvin Jaeger
North Dakota Secretary of State

David Jefferson
California Internet Voting Task Force/ Compaq Systems Research Center
Ronald Reagan Library, April 12, 2001

Carolyn Jefferson-Jenkins
League of Women Voters
LBJ Library, May 24, 2001

William Jenkins
General Accounting Office

Kathy Johnson
The United States Access Board

Bill Jones
California Secretary of State
Ronald Reagan Library, April 12, 2001

Pamela Karlan
Stanford Law School
LBJ Library, May 24, 2001

Stephen Kaufman
Smith Kaufman LLP

Kevin Kennedy
Wisconsin Elections Board

Carolyn Jefferson Jenkins
Joan Konner

Alexander Keyssar
Duke University
The Carter Center, March 26, 2001

Brad King
Office of the Minnesota Secretary of State

Jean-Pierre Kingsley
Elections Canada
Gerald R. Ford Library, June 5, 2001

Stephen Knack
American University

Joan Konner
Columbia University Graduate School of Journalism
Gerald R. Ford Library, June 5, 2001

Jon Krosnick
The Ohio State University

Linda Lamone
Maryland State Board of Elections

Richard LaVallo
Advocacy Inc.

Jan Leighley
Texas A&M University

R. Doug Lewis
The Election Center
Gerald R. Ford Library, June 5, 2001

Matt Lilly
Danaher Controls

Keith Long
Hart InterCivic

Susan MacManus
University of South Florida
The Carter Center, March 26, 2001

Ruth Mandel
Eagleton Institute of Politics
The Carter Center, March 26, 2001

Sheilah Mann
American Political Science Association

Jeff Manza
Northwestern University

Mitch McConnell
United States Senator for the State of Kentucky
written submission

Conny McCormack
Los Angeles County, Registrar-Recorder/County Clerk
Ronald Reagan Library, April 12, 2001

Gary McIntosh
Office of the Washington Secretary of State

Leigh Middleditch, Jr.
McGuire Woods

Alice Miller
District of Colombia Board of Elections and Ethics

Julie Moore
Elections Operations, King County, Washington

John Mott-Smith
Office of the California Secretary of State

Michael Neblo
University of Chicago

Peter Neumann
SRI International

Bob Ney
Member of the United States Congress for the Eighteenth District of Ohio
written submission
Gerald R. Ford Library, June 5, 2001

Stephen Nickelsburg
Hunton & Williams

Colm O'Muircheartaigh
National Opinion Research Center

Norman Ornstein
American Enterprise Institute for Public Policy Research
LBJ Library, May 24, 2001

Sharon Priest
Hilary Shelton
Scott Thomas

Lee Page
Paralyzed Veterans Association

Robert Pastor
Emory University
Gerald R. Ford Library, June 5, 2001

R. Hewitt Pate
Hunton & Williams

Cathy Pearsall-Stipek
Auditor, Pierce County, Washington

Carol Petersen
General Accounting Office

Katherine Pettus
Columbia University

Deborah Phillips
Voting Integrity Project
The Carter Center, March 26, 2001

Trevor Potter
Caplin & Drysdale

G. Bingham Powell
University of Rochester

Sharon Priest
Arkansas Secretary of State
LBJ Library, May 24, 2001

Mark Pritchett
Collins Center for Public Policy, Inc.
The Carter Center, March 26, 2001

Cameron Quinn
State Board of Elections,
Commonwealth of Virginia

Wendy Rahn
University of Minnesota

Jack Rakove
Stanford University
The Carter Center, March 26, 2001

Joseph Rich
United States Department of Justice, Civil Rights Division
LBJ Library, May 24, 2001

Eric Riedel
University of Minnesota

Ron Rivest
Massachusetts Institute of Technology

Susan Roth
The Ohio State University
Ronald Reagan Library, April 12, 2001

Eric Royal
United Cerebral Palsy

Janet Ruggiero
Office of the Rhode Island Secretary of State

Larry Sabato
University of Virginia
The Carter Center, March 26, 2001

Roy Saltman
Independent Elections Consultant
written submission

Anthony Salvanto
University of California, Irvine

Paul Schumaker
University of Kansas

Ted Selker
Massachusetts Institute of Technology

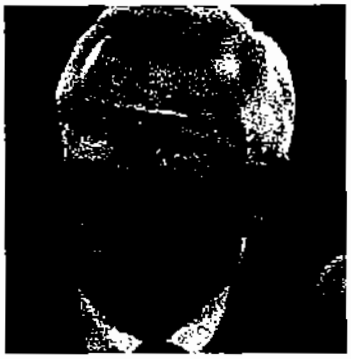
Hilary Shelton
National Association for the Advancement of Colored People
LBJ Library, May 24, 2001

W. Phillips Shively
University of Minnesota

Howard Silver
Consortium of Social Science Associations (COSSA)
written submission

Margaret Sims
Federal Election Commission

Liz Smith
Furman University



Michael Traugott
Lance Ward
Admiral Stephen Yusem, Ret.

Richard Soudriette
International Foundation for Election Systems
Gerald R. Ford Library, June 5, 2001

Alfred Speer
State of Louisiana House of Representatives

Martin Stephens
State of Utah House of Representatives

Eliot Spitzer
New York Attorney General
written submission

Ralph Tabor
National Association of Counties

Clyde Terry
New Hampshire Developmental Disability Council

Abigail Thernstrom
United States Commission on Civil Rights
written submission

Christopher Thomas
Michigan Department of State Bureau of Elections
Gerald R. Ford Library, June 5, 2001

Rosita Thomas
Thomas Opinion Research

Scott Thomas
Federal Election Commission
Gerald R. Ford Library, June 5, 2001

Daniel Tokaji
American Civil Liberties Union Foundation

Mischelle Townsend
Registrar of Voters, County of Riverside, California
Ronald Reagan Library, April 12, 2001

Michael Traugott
University of Michigan
Gerald R. Ford Library, June 5, 200

Fran Ulmer
Alaska Lieutenant Governor
written submission

James Villiesse
City Clerk of New London, Wisconsin

Lance Ward
Oklahoma State Election Board
LBJ Library, May 24, 2001

Tracy Warren
The Constitution Project

Geraldine Washington
Los Angeles NAACP

Maxine Waters
Member of the United States Congress for the Thirty-Fifth District of California
Ronald Reagan Library, April 12, 2001

Martin Wattenberg
University of California, Irvine

Bob Williams
United Cerebral Palsy

Brit Williams
Kennesaw State University

Raymond Wolfinger
University of California, Berkeley

Stephen Yusem
Rear Admiral, (Ret.), Reserve Officers Association of the United States
Gerald R. Ford Library, June 5, 2001

Bob Zeni
Voting Experience Redesign Initiative
written submission

See pg 6

AUDITABILITY OF NON-BALLOT, POLL-SITE VOTING SYSTEMS

by
Roy G. Saltman, M.S., M.P.A.
Consultant on Election Policy and Technology
rsaltman@alum.mit.edu
Revised: August 24, 2003

Abstract

The history of the use of non-ballot voting systems in the US is briefly described. The background of a current controversy is also noted. The differences between DREs as currently used and Internet voting are discussed. The voting process as a human system involving people, procedures and activities as well as machines is stressed. Alternative systems employing ballots are described, and their advantages and disadvantages as compared to DREs are discussed. Specific machine design changes and administrative changes in the testing and use of DREs are recommended.

1. Background

The question of implementation of audit trails in non-ballot, i.e., direct-recording electronic (DRE) voting systems, is not new. It was discussed extensively in 1988 [Saltman, R., 1988, pp. 40, 41, 112-114] and a requirement for part of the recommendations proposed in 1988 was included in the Federal Election Commission standards of 1990 [Federal Election Commission, 1990, p. 18]. Recently, the topic arose again in connection with the desire of officials of Santa Clara County, California, to procure DRE systems for use by the voters of that county. Opponents of this procurement, led by David Dill, professor of computer science at Stanford University, proposed a requirement for a paper audit trail that is "voter verified." That is, a paper record of the ballot would need to be produced by the DRE voting unit and approved by each voter before the ballot is cast. This demand of Dill and other computer scientists follows the recommendation of Rebecca Mercuri, professor of computer science at Bryn Mawr College, that has been presented on several occasions [e.g., Mercuri, R., Neumann, P., 2003, p. 40].

Following a request by officials of Santa Clara County for an opinion from the state, the Office of the Secretary of State of California undertook a study and issued a report [Secretary of State's Ad Hoc Touch Screen Task Force, 2003]. The Task Force made several recommendations to improve the security and integrity of voting systems, and noted the new federal requirement that there must be a paper record for each ballot cast. The federal statute is interpreted to mean that the individual records could be printed in bulk from electronic records after the polls are closed. However, the Task Force stated:

> "For technical and logistical reasons there is no support to have the printing of this permanent paper record done at the time the ballot is cast ..."

Thus, the state did not accept the demand of the computer scientists, but allowed that a county could purchase systems with this feature, if it so chose. The purpose of the discussion below is to further elaborate the arguments on both sides and to consider improved mechanisms that would increase voter confidence in the results produced by DRE voting machines.

2. Lever Machines:

The use of non-ballot, poll-site voting systems in the US goes back over one-hundred years. In 1899, the US Congress approved the use of non-ballot mechanical lever machines in voting for candidates for the US House of Representatives. After that, the use of lever machines spread widely and, for the general election of 1960, the last Presidential election before the start of adoption of punch-card voting, it was reported that 55 % to 60% of the voters in this nation used them. In the Presidential election of 2000, they were used by about 19 % of US voters. Interestingly, no concerted effort by computer scientists was ever mounted, in the roughly forty years that computer science has been a profession, to persuade election officials not to use lever machines, despite their clear failure to provide an audit trail. This writer, however, has discussed the difficulties of these machines [Saltman, R., 1988, pp. 26-29].

The complete auditability of mechanical lever machines is not possible. Individual voter-choice sets, i.e., the groups of particular votes cast for all contests by each individual voter, are not retained. Consequently, there can be no demonstration of the complete content of any voter's set of selections. Only the sums of votes cast by all voters for each candidate and issue alternative are stored. As a result, it is not possible to determine the cause of a vote recorded as not cast in a contest without a close examination of the internal workings of the particular machine that was used. It may be that a voter chose not to cast the vote in question, but it may be that the voter attempted to cast it but the machine, because of an internal malfunction, failed to record it. (The machine failure may have been due to a structural defect that gradually appeared without being noticed on account of a lack of adequate maintenance, but it is possible that the malfunction was due to malicious human action.)

3. DREs:

These machines began to be used in1974. An experimental model was referred to in a report in 1975 as an "electronic vote summarizer" [Saltman, R., 1975, p. 13, 14]. There are three basic types used in the United States: pushbutton, micro-switch and touchscreen. The first DREs used pushbuttons to replace the levers. The next improvement was the use of micro-switches, activated by voter touch, placed beneath a hard but somewhat flexible surface on which the choices were presented. The newest development involves the presentation of candidates' names on an electronic monitor within areas of the screen sensitized to touch. A touch of the screen at the location in which a candidate's name is presented causes the computer to respond programmatically. All three of these types continue to be used. DREs became popular slowly; in 1988, they were used by only 2.7 % of the US electorate, but in 2000, 10 % of all voters used them. As a result of the debacle of punch card voting in the 2000 Presidential election in Florida and the subsequent passage of the (Federal) Help America Vote Act (HAVA), their usage is likely to increase significantly. For example, Georgia used them throughout the state in 2002. Maryland has decreed that any of its 23 counties that are not using them now will eventually use them at poll sites; mark-sense ballots will be used for absentee voting. Baltimore city, Montgomery County and Prince Georges County, three of Maryland's most heavily populated jurisdictions, used DREs in 2002.

Since the specification of the 1990 Federal Election Commission standards that "electronic ballot

images" (their phraseology for "voter-choice sets") be retained within the machines, it is very likely that all DREs produced since then have this capability. Additional design features should be mandated, and additional testing and system assurance operations should similarly be required. These concerns are addressed below.

4. Voting Over the Internet:

This presentation does not concern voting over the Internet. It concerns only poll-site voting; that is, voting in which individual votes are **not** communicated electronically outside of the physical location in which they are cast in order to be summarized with other votes for the same candidate. Internet voting involves additional levels of risk and additional controls beyond the scope of this paper. The risks of Internet voting should not be used to taint the use of DREs by combining the latter with the former as "electronic voting" and by giving the impression that the unique difficulties of Internet voting apply also to DREs. There is no reason for DREs to use the Internet during operations, and those recently purchased for Maryland will not do so, despite the implication to the contrary in a recent study [Kohno, T., Rubin, A. et al, 2003]. That study also attempted to analyze DRE software separated from the election system of which it apart - a fatal error. See **Section 5** about the systems concept.

5. Voting as a Human System:

It must be understood that voting is a complex system involving people as well as machines. Concerns for the system cannot be reduced to the single issue of correctness of software, although that is certainly important. Information systems used by both business and government are tools that people use to assist them in performing their duties and achieving results defined by organizational management. Some of the criteria for success of the particularly complex system for voting are these: (1) the voters are easily able to convert their choices exactly as they intend into commands to the system; (2) the system processes the voters' choices correctly; and (3) there is public confidence in the results produced by the system. Mistakes can be made, and often the mistakes are made by people - the voters or the administrators.

The integrity of the information system for voting involves considerably more that just correctness of software. The latter issue as the only essential one was first raised in *The Los Angeles Times* in 1969 and in *The New York Times* in 1985. The story made the front pages of major newspapers twice because the idea of software manipulation was sensationalistic. The presentations' positive value was that they sensitized policy makers to the potential threats to administration of elections and generated studies on the reductions of threats. The negative value of the stories was that the special focus detracted from the necessary view of how to improve the entire process from a systems perspective.

In 1989, I was asked by the International Association of Clerks, Recorders, Election Officials and Treasurers (IACREOT) to present, at their annual meeting that year in San Diego, my answers to three specific questions. The first of the questions was the following:

> What ways are there that would make it possible to "rig" an election using computers, i.e., Voting Machines, Direct Electronic Voting, Punchcard and Optical

Scan Equipment? [Saltman, R., 1989, p. 1]

My response continues to be pertinent, because the same question constantly arises in essentially the same context. Here is part of my answer:

> "Election administration is a **system** that consists of four elements: (1) people, (2) established procedures, (3) devices and machines, and (4) activities. Election administration activities should be undertaken, according to established procedures, by the people using the devices and machines. Before there were computers, there were other devices and machines used in election administration and, consequently, some procedures were different.
>
> "However, the election administration process was a **system** then; it remains a **system** now. The use of computers has not changed that. The process remains a system that is managed and carried out by people, that is, election administrators. Election administrators, not vendors, not manufacturers, not other contractors, are responsible for the accuracy of the results produced, in order to assure that the "consent of the governed" is truly achieved.
>
> "The reason that I have stressed that election administration is a system is that **it is not possible to separate the question of manipulation of computers for election "rigging" from considerations of the system of which the computer is a part.** If a computer has been used to "rig" an election, either the procedures used to carry out the election were inadequate, or the people managing and carrying out the activities did not follow established procedures. Thus, instead of telling you what ways there are to use a computer to "rig" an election, I must tell you what proper and effective procedures there are, to be used by you, the election administrators, to assure accurate results that correctly reveal the choices of the voters.
>
> "These proper and effective procedures need to include those used to (1) **acquire** hardware and software according to performance specifications, (2) **check out** hardware and software for logical correctness, integrity and reliability, (3) **protect** acquired hardware and software against unauthorized access, and (4) **effectively employ** hardware and software in election operations."

6. <u>Vulnerabilities of Ballot Systems:</u>

<u>Ballot-counting voting systems</u> are not necessarily less vulnerable to mistakes and fraud than non-ballot systems. In fact, one of the major reasons that mechanical lever machines were adopted in the US in the early 20th century was because of significant ballot frauds. Two vulnerabilities of these systems are:

(1) **Ballot-readers are not totally accurate**, particularly when attempting to read marks or punches made by real humans. The difficulties in punch card systems need not be elaborated; they are too well known. Voters using mark-sense systems may make marks that are too light to be accurately sensed, may make smudges at unintended voting positions that may be sensed by mistake or may use

an incorrect writing instrument that fails to register their votes. They may make marks outside of the assigned areas that the machine can sense, requiring an "intent of the voter" manual analysis. Furthermore, mark-sense readers may be reduced in sensitivity by dust from ballots or from the environment.

(2) **Ballots may be miscounted,** even if there is no ballot-stuffing. In Florida, in the 2000 Presidential election, several counties using ballot-counting systems found significant numbers of additional ballots in their automatic machine recounts. In one county, a poll station manager, with the ballot cards in the trunk of her car, stopped off to see a friend before delivering the ballots and forgot about them. Nassau County's recount was different (adding a net 71 votes for Gore) than its original count, but the County Canvassing Board decided that their first count was correct, not their second one. As a result, Gore's contest of the certified vote count separately included a demand for another recount in Nassau County. When the US Supreme Court summarily and prematurely ended the statewide recount ordered by the Florida Supreme Court, a result was that a true determination of the Nassau County results was never completed.

7. Vulnerabilities of DREs:

DRE counting systems have the vulnerability that there is no hard-copy audit trail. It is important to note that a hard-copy ballot, created by a programmed computer even if the input is provided by the voter, does not automatically constitute a document-ballot that is independent of the computing machinery. As I stated in 1988, "the fact that the voter can see his or choices on a display, or even receives a printout of the choices made, does not prove that those were the choices actually recorded in the machine to be summarized for generating the results of the election" [Saltman, R., 1988, p. 41]. **A printout or hard-copy ballot produced by the machine is not independently created by the voter; it is subject to the correctness or incorrectness of the computer program that created it.** With electronic non-ballot voting systems, the computer program actually casts the votes. The computer may cast votes that differ from the voter's intent if the program was written to carry out that insidiously incorrect activity [Saltman, R., 2003, p. 133].

8. Value of a Printout for DREs:

If the intention of a printout from a DRE machine is to give the voter a sense of confidence that his or her vote was properly cast and properly processed, that confidence would be false. Due to the fact that the printout is created by the computer and is not a document-ballot, such a printout is a sop to the layperson ignorant of the inner workings of computers. There must be better ways of providing the necessary confidence to the voters. It is the intention of this paper to propose some.

9. The Ballot Solution to the DRE Auditability Problem:

A DRE voting unit may be considered as three subunits. The first subunit may be called the Vote-Entry Section (VES) and the second subunit may be called the Vote-Summarizing Section (VSS). The input to the VES are the voter's choices, typically entered through the voter's fingers acting on pushbuttons, micro-switches, a keyboard, a mouse or a touchscreen, and its outputs are the voter's choices converted to an electronic form (voter's electronic ballot image or EBI). The inputs to the VSS are the outputs from the VES for each voter, and the output of the VSS is the summary of votes cast on the DRE. The third subunit, the Ballot Image Storage Unit (BISU) also receives the

EBIs from the VES and permanently stores them in a secure manner so that they cannot be overridden.

Suppose that the VSS were separated from the other two subunits, but was still in the same physical location, so that the output of the VES would not go directly to the VSS, but instead would go to a printer that would generate a mark-sense ballot. The mark-sense ballot could be created in a language of the voter's choosing, assuming the language were pre-programmed, meeting the multi-language requirements of the Voting Rights Act. This mark-sense ballot, because it would be machine-generated, would have a very high likelihood of being read correctly by a mark-sense reader. Suppose, then, that the voter had the opportunity to review the mark-sense ballot and found it to mirror exactly what the voter intended. Then the voter could deposit the mark-sense ballot in an **independently programmed** VSS through a mark-sense ballot reader. Then, if "the cast ballot becomes the only source of vote-recording and counting, it would be considered a document-ballot. Then the voting system would not be a non-ballot system" [Saltman, R., 2003, p. 133].

A system such as this has been proposed by Alan Dechert for use in California. This type of system would be acceptable to those demanding a "voter verified" audit trail. It is not a DRE system. Is it still possible, with additional controls designed into the machine and the system, to allow for the use of a DRE with confidence that it is providing the correct results? Consider the following recommendations.

10. <u>The Human System Solution to the DRE Auditability Problem:</u>

The ballot solution presented above eliminates the "intent of the voter" issue because of the machine-generated ballots, However, it includes an extra printer for each VES and an extra ballot-reader for each VSS. It negates also the value of a DRE because it uses paper ballots. Recent studies of the economics of different system types demonstrate that the cost of paper ballots that cannot be re-used is significant. That is, the operational cost of a ballot-using system must include the paper ballots for each election, a cost that does not have to be borne by DRE systems. The operational cost of ballots may, over time, cause total system costs of ballot systems to be greater than that of DRE systems.

10.1 <u>The DRE Design Part of the Solution:</u> If DRE systems are to be used without the production of hard-copy ballots, the problem of an audit trail that can be trusted must be solved. The following design features are recommended. They are specifically proposed with a view toward improving human factors and increasing public confidence in the results produced by the system. Whether or not the proposed features make the DRE acceptable is a decision to be made by the elected political leaders of the jurisdiction purchasing the voting system.

(1) **Resetting of each machine following the completion of each voter's effort:** Each completion of the voting process by a voter should result in the machine's inability to receive any more commands until reset for the next voter. It is likely that this activity is now being carried out with most DRE systems, but is restated here because of the claim of the study by Kohno, Rubin et al. that implied that one voter could continually use the machine to insert many votes.

(2) **Direct report to the voter on his or her contribution to the count of votes:** A significant concern of computer scientists appears to be the inability of the voter to discern the fact that his or her vote was counted. With the use of precinct-located mark-sense ballot systems, when the voter deposits his or her ballot in the reader, a counter on the machine visible to the voter will increase by "one," demonstrating to the voter that the ballot was added to the pile of ballots already received. In that system, the voter has no information as to what happens to the ballot after it is deposited. It may be maliciously altered or replaced by a counterfeit, but the fact that the count of ballots is increased by "one" seems to be satisfactory to the computer scientists who claim to know what constitutes voter confidence. Therefore, it is proposed that the DRE machine, as a result of the voter reporting "all voting complete," should present a final screen showing to the voter the previous number of votes received by the machine and that number increased by "one." That action will demonstrate to the voter that his or her votes were added to those already received.

(3) **Recording of EBIs and recounting on a separately programmed machine:** DRE machines provide for the retention of EBIs in the BISU. The recording should be on a removable diskette that can be inserted in a separate independently programmed machine for recounting. Thus, California's requirement that one-percent of the precincts be recounted could be met. The retention of the EBIs allows also for their printout to meet the new HAVA requirement.

(4) **Reconciliation of all votes and undervotes:** All undervotes should be positively recorded for purposes of reconciliation. (Overvotes are not possible on a DRE). This is not done now, but I previously recommended it [Saltman, R., 1988, p. 112, 113]. Reconciliation should be accomplished by designing into the internal logic of each VES, a special "no-vote" bit for each contest. (We assume, for simplicity, only 'vote-for-one' contests. The solution is easily extended to 'vote-for-N' situations.) In typical current systems, there is, in the VES internal logic, a "vote" bit for each candidate that is set to "zero" when the machine is activated for a new voter. When a voter selects a candidate, the "vote" bit for that candidate is set to "one." If the voter fails to vote in the contest, no bit is set to "one" in the voter's EBI, and when the voter is finished voting, no "one" bit is recorded or transmitted to the VSS for that contest.

As proposed here, each contest would have, in addition to a "vote" bit for each candidate, a single "no-vote" bit which would be set to "one" when the VES is reset for a new voter. If the voter votes in the contest for any candidate, the "no-vote" bit is reset to "zero." If the voter has completed the voting process and has not voted in a contest, the value of the "no-vote" bit, which should still be a "one" is transmitted to the VSS in the voter's EBI. This process provides for the transmission of one "one" for every 'vote-for-one' contest and provides that the number of "ones" in each EBI sums to the number of vote-for-one contests on the ballot. It also allows for the use of an additional results line that specifies the number of "no-votes" for each contest. The reconciliation occurs in that, for the results of every contest, the sum of the number of votes for candidates plus the number of "no-votes" always equals the number of voters that have used the machine. The number of votes not cast in each contest should be printed, along with the votes cast for each candidate or issue alternative. This reconciliation is intended to further public confidence in the results.

(5) **Second-chance voting:** The addition of the "no-vote" bit for each contest in the VES provides

the information to allow the machine to report to the voter, if the "all voting complete" indicator has been prematurely activated, that the voter has not voted all contests. In a touchscreen system, the information available will allow the machine to report on the screen the highest contest not yet voted, and should allow the voter to continue voting, if that is desired. This is of particular value to the voter if the voter has mistakenly activated the "all voting complete" indicator too early as an unintended reflex action. In the use of Internet web sites or with application programs, many systems will respond to a user who mistakenly activates a command with a screen or display that permits the user to retract the command, e.g., with a "cancel" option. Election administrators should do no less for voters.

(6) **Voter's review of choices:** The DRE should be designed so that the voter may review choices in each contest before completing the voting process. With a full-face DRE, the voter needs only to look at the choices clearly presented in front of him or her. With a monitor screen, the voter needs to be able to return to the screen for any contest. The capability to do that must be clearly shown to the voter. Human-factors research could investigate the best manner to show the summary of choices to the voter. The demand that this information should be on paper rather than just on the full-face DRE or on a computer monitor is puzzling. It harks back to the time when computers first began to be used in the 1950s and 1960s, and skeptics re-calculated results on electro-mechanical machines because they did not trust the computer. Now we have better methods of assuring software correctness.

(7) **Naming of the "All Voting Complete" indicator:** This indicator should not be called "Vote." That name is confusing in its similarity with the completion of action on a particular contest. A more definitive name such as "All Voting Complete" needs to be used.

(8) **Connector for entry of test votes:** There should be a physical connector on the VES which allows for entry of a series of electronic test votes of any number, as if many voters had voted on the machine. The entry point should replace the voter inputs that would fill the temporary storage location with voter's selections in the VES, so that the recording of the selections in the BISU and the summarization process of the VSS may be checked. I have seen a device that generates test votes and exercises a DRE through a connector, as I have proposed. Thus, it has already been done for at least one system. Note that the testing will not test the correctness, in the VES, of the transference of the voter's choices to the temporary storage locations in which the choices are first stored. This part of the VES would need to be separately checked.

10.2 The Software and Hardware Assurance Part of the Solution: All software and hardware to be used must be thoroughly checked out upon delivery following procurement, and then again in preparation for any election. As the integrity of elections using DRE equipment depends on software and hardware correctness, testing must be thorough. Software should be required to be written so that, in preparation for any election, the logic of the software remains unchanged and only blanks are filled in to adapt or specialize the software for a particular election. Software testing must assure the lack of hidden loops that are intended to be exercised only at a particular time or only when a particular value is inserted in a specialization process. My reports of 1975 and 1988 are filled with recommendations of procedures for carrying out systems assurance.

10.3 Audit Trail for Software Handling: It is essential that specifications be written and followed as to the manner in which all software and storage units containing software are to be handled, tested and transported to assure integrity. That is, an audit trail needs to be established for the handling of software. These procedures, if well written and carried out, will prevent the rumors of software manipulation that flourish in an atmosphere of lack of knowledge and lack of specificity.

10.4 The Administrative Implementation of Assurance: It is desirable that each state establish its own system integrity process beyond that established through the NASED-sponsored Independent Testing Authorities. Additional testing may need to be provided. Each state may wish, further, to establish a Voting System Assurance Advisory Committee, with a Computer Technology Subcommittee, that will recommend system assurance procedures. The latter group should be able to help devise the best methods for testing of software to assure correctness and the absence of malicious code. The establishment of these administrative structures and the publication, for public dissemination, of what is being done, will provide the public confidence in the operation of elections that is currently lacking.

11. Summary:

Possible changes in the design of DRE units and the administration of the vote-counting system have been proposed. The intention of these proposed changes is to improve the auditability of DRE systems and thereby to improve public confidence in the results produced. An alternative ballot-counting system has been discussed, and its differences with DRE systems have been noted.

The assurance of public confidence in vote-counting is an issue of systems design and assurance; it is not limited to a single palliative measure, e.g., the provision of hard-copy ballots in DRE systems. Assurance of public confidence is not a new issue. For example, my 1975 report contains the following:

> "The assurance that steps are being taken by election officials to prevent unauthorized computer program alteration or other computer-related manipulations remains, nationwide, a continuing problem for the maintenance of public confidence in the election process" [Saltman, R., 1975, p. 4].

The solution to the issue of public confidence requires reviewing the vote-counting information system from a multi-disciplinary perspective. Public administration, human factors concepts, information systems engineering, internal auditing, public communications, and other disciplines are important to apply, as well as computer science.

12. References:

Federal Election Commission, 1990, Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems, Washington, DC.

Mercuri, R., Neumann, P., 2003, "Verification For Electronic Balloting Systems," in Gritzalis, D.

(ed.), Secure Electronic Voting, Kluwer Academic Publishers, Boston, MA.

Kohno, T., Rubin, A., Stubblefield, A., Wallach, D., 2003, Analysis of an Electronic Voting System, Information Security Institute, Johns Hopkins University, Baltimore, MD.

Saltman, R., 1975, Effective Use of Computing Technology in Vote-Tallying, NBSIR 75-687, March, 1975 (reprinted as NBS SP 500-30, April, 1978), National Bureau of Standards, Washington, DC (now National Institute of Standards and Technology, Gaithersburg, MD).

Saltman, R., 1988, Accuracy, Integrity, and Security in Computerized Vote-Tallying, NBS Special Publication 500-158, National Bureau of Standards, Gaithersburg, MD, (now National Institute of Standards and Technology, Gaithersburg, MD).

Saltman, R., 1989, Accuracy and Integrity of Computerized Vote-Counting: Answers to Three Fundamental Questions Posed by Election Administrators, Presentation to IACREOT annual meeting, San Diego, CA, June, 1989.

Saltman, R., 2003, "Public Confidence and Auditability in Voting Systems," in Gritzalis, D., (ed.), Secure Electronic Voting, Kluwer Academic Publishers, Boston, MA.

UNIVERSITY OF CALIFORNIA, BERKELEY

BERKELEY • DAVIS • IRVINE • LOS ANGELES • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

UC DATA
Data Archive & Technical Assistance

2538 CHANNING WAY # 5100
BERKELEY, CALIFORNIA 94720-5100
(510) 642-2337
FAX (510) 643-8292

May 2, 2001

To: Alan Dechert
From: Henry E. Brady
Professor of Political Science and Public Policy
Director, Survey Research Center and UC DATA
Re: A Proposal to Improve Voting Systems in California

I am very enthusiastic about working together with you in a joint project to improve voting systems in California. I believe that our interests and capabilities are quite complementary, and the following integrates your interest in developing alternative PC-based voting systems with my interest in understanding the patterns of over and under-votes in California in order to find ways to reduce them to the bare minium. The project proposed below, I believe, will provide invaluable information and some very useful models for improving voting systems in California. Indeed, this project is thoroughly consistent with the University of California's origins as a land grant university and with its traditions of working to make contributions to the state of California.

Outline of a Proposal -- You have proposed a voting system development project that would be PC based, open source, and inexpensive. This idea has real and substantial merit, and it is definitely worth exploring. In fact, as you know, Roy Saltman,[1] the author of the two best known books on computerized voting, has agreed to work on this project, and he is enthusiastic about developing the kind of system you have proposed. The Survey Research Center of the University of California at Berkeley, with its long tradition of helping the state of California solve its data collection problems, is an excellent place to undertake this kind of research and development effort. In effect, the task of tallying votes is a very specific kind of data collection problem with features that are very familiar to our professional staff. The Survey Research Center provides a range of data collection services which address problems that are similar to the ones that we will confront in this project. Through the SRC's Survey Services Facility, we design questionnaires and conduct surveys. The design of questionnaires, especially self-administered questionnaires, is very similar to the problem of designing effective ballots, and conducting surveys leads to problems of obtaining reliable information and insuring confidentiality that are central to the vote tallying task. Through our Data Archive and

[1] Roy G. Saltman, *Accuracy, integrity, and security in computerized vote-tallying*, Gaithersburg, MD: U.S. Dept of Commerce, National Bureau of Standards, 1988.

Roy G. Saltman, *Effective use of computing technology in vote-tallying*. Washington, D.C.: Clearinghouse on Election Administration, Office of Federal Elections, General Accounting Office.

Technical Assistance program (UC DATA), we develop computerized data collection systems and we analyze the data produced from these systems for integrity and reliability. Again, these problems are parallel to the difficulties faced by computerized vote tallying systems. Through our work, we are also knowledgeable about problems of privacy and confidentiality, and we have done studies for the National Academy of Sciences and the State of California on these issues. For this project, your expertise in developing software and hardware solutions for human-machine interactions is an essential addition to our capabilities.

In order to provide the State of California with the best possible information about its current and prospective vote tallying systems, we propose a study that completes the following five steps:

(1) Assessment of the Current Situation -- Assess the current state of the vote counting system in California by using already available statistical data and by generating new data through surveys and interviews of election officials. This study will not only study the role that voting systems themselves play in the effectiveness of vote counting, but it will also study the administrative factors that lead to effective vote counting. As you know, I am already deeply involved in these kinds of studies, and I can take the lead.

(2) Delineation of Technological Needs -- Delineate the common and unique vote counting needs of California's 58 counties in order to determine what kinds of technological improvements could improve the effectiveness of vote counting in California. This step will require a survey of the 58 counties and in-depth interviews with election officials from all parts of California. The SRC is well-equipped to complete this task.

(3) Development of a Prototype System -- Develop a prototype system that is PC based, open source, and inexpensive as a way to learn more about the needs of the counties and to determine the feasibility of alternatives to the currently available commercial systems. The work on this element will interact with the efforts in all other areas. By actually developing a system, we will learn more about the technological issues involved, and we will be placed in a situation where we must be responsive to the election officials who must ultimately cope with the problems of counting votes.

(4) Work with the Private Sector -- Study the strengths and weaknesses of the available systems by working with vendors. We will also work to encourage the private sector to develop new technologies that will improve our voting systems. This step will involve meeting with vendors, acquiring and studying their products, and providing feedback to them on the needs that we find in California's counties.

(5) Conference with California Officials to Present our Results – Once we have made substantial progress in steps 1–4, we will have a conference involving state election officials and others to discuss our preliminary results.

I have been working on items (1) and (2), and you have been working on items (2) and (3). Item (4), will ensure that we make the best possible use of the options currently available from the private sector. I think that the main task involved in completing (4) is meeting with the vendors and discussing their systems. We will jointly organize the conference described in (5).

Completing Steps 1 and 2 – Assuming that funding would begin by June 1st, I believe that a *detailed draft* of a report for step 1 and step 2 could be completed by the late Fall of this year. This step would involve the following kinds of analysis:

– A statistical report using available data from the California Statewide Database

– Collection and analysis of undervote and overvote data at the precinct level from as many counties in California as possible

– A survey of all 58 county election officials to learn about their procedures and approaches to counting ballots

– In-depth interviews with a large number of county election officials

– Planning a conference to present results and receive feedback.

Although the SRC will do much of the work on steps 1 and 2, I believe that you will want to be involved in some of these tasks, especially the in-depth interviews of county election officials.

Completing Steps 3 and 4 – You will be the project director for these steps, and you will work with me, my staff, and graduate and undergraduate students. As we discussed, the central task will be to develop a PC-based, open source, and inexpensive voting system. In addition to setting up a polling place mock-up where the public can try out PC-based voting, we will produce a report or reports incorporating data collection and analysis covering the following topics:

• Multi-use equipment verses dedicated equipment. Can we identify where PCs might be used between elections?

• Open source software for vote recording verses proprietary systems

• Open source software for vote tabulation verses proprietary tabulation software. Can we enable voters to check tabulation using precinct-level data?

• Printing completed ballot verses no printed ballot at all

• Using the Internet to publish precinct-level election results. Would it also be feasible to publish each ballot?

- Vulnerability to Election Day power outages.

- Can we enable voters to vote at any polling place?

- What other equipment is needed (e.g., furniture) to accommodate these systems at the polling places? How expensive are these items to purchase, transport, and store?

- How are write-in votes handled?

- How vulnerable are these systems (these systems = PC based systems and DREs) to malicious insiders?

- How vulnerable are these systems to malicious outsiders?

- Should the voter get a printed receipt that includes details of how he or she voted? Or, should a receipt only include a ballot number? Or, is no printed receipt necessary?

- Since the PCs are standalone, how do we transfer the votes from the individual voting machines to a more central location?

- Should votes be tabulated and published at the precinct level before they go to a more central location?

- How can election results be fully audited and certified on these systems?

- How well do these systems work for visually impaired voters?

- How well do these systems work for non-English voters?

- How do these systems work with absentee and provisional ballots?

- Is it necessary to have a paper ballot backup in case voters can't or don't want to vote on the electronic systems? How could this be accomplished?

- Compare initial costs of these systems. Compare life-cycle costs of these electronic systems, and compare to existing non-electronic systems. Compare multi-use PC based systems with dedicated PC based systems and dedicated DREs.

- How difficult is it to recruit and train pollworkers to work with these systems?

- What are some of the best alternatives for absentee ballot tabulation for counties using DREs or PC based systems in the polling places?

• Provide a method to determine the percentage of the voters that can use a mouse-based system at each polling place.

In order to insure that we are addressing these questions in the most effective manner, we will have periodic reviews of progress by an internal SRC board of experts including myself, Dr. Fred Gey (Assistant Director for Technical Services and an expert in computing technologies, information retrieval, and database management), Dr. Tom Piazza (Head Statistician and an expert in survey design and statistical issues), and Dr. Donna Eisenhower (Director of Survey Services and Senior Research Scientist and an expert in survey design and data collection methodology). We will also bring in outside experts such as Dr. Roy Saltman as we go along.

Completing Step (5) – After we have completed the draft report, we will have a conference of California election officials to discuss both the report and your progress on a prototype PC system.

Proposed Budget – The SRC cost of completing these steps would be to support some of my time, to support some time of my professional staff to help manage and direct the project, to support four graduate and/or undergraduate students for twelve months at 100% during the summer and 50% during the school year, and to cover miscellaneous costs. The costs would be:

– *Principal Investigator* -- Total $19,200. Henry E. Brady, Professor of Political Science and Public Policy, Director, Survey Research Center and UC DATA. One month of my time; Salary plus benefits at $19,200.

– *Technical Lead* – Total $150,000. Alan Dechert, ¾ time for one year (1500 hrs) at $100 recharge rate, $150,000.

– *Project Management* -- Total $21,800. Twenty percent of the time of one member of SRC professional staff (that is, one day a week) to oversee the project. Salary plus benefits at $21,800.

– *SRC Professional Staff Technical Oversight* – Total $10,000. Regular monthly meetings of Dr. Donna Eisenhower, Dr. Tom Piazza, and Dr. Fred Gey with the PI, Technical Lead, and others to ensure proper technical direction and to provide help on technical issues as needed.

– *Four Graduate/Undergraduate students* – Total $107,000. Each student at 3 summer months at 100% and 6 school-year months at 50% for a total of 5000 hours. (500 hours for each person during the summer and 750 hours during the school year.) Each one would cost approximately $17 per hour plus tuition/fee remissions. (The University requires that we charge these tuition/fee remissions.) The total should be something like $87,000 for wages, 17,000 for fee remissions, and $3,000 for benefits.

– *Technical Consultants* -- Total $40,000. Consultants on various topics including – (These may be external consultants or UC Berkeley Professors)

Computers and voting systems – E.g., Roy Saltman

Conduct of Elections—E.g., Curtis Gans

Conduct of Experiments –E.g., Professor Rob Maccoun

Other Consultants – Experts on software and government

– *Supplies, Expenses, Travel* – Total $15,000. Expenses for telephone, office supplies, duplication, mailing, University liability program, $4,000. Expenses for travel $10,000 including trips for consultants and extensive travel within California to interview election officials. (There will be site visits to many of the 58 counties and telephone interviews with officials from around the state.)

– *Equipment* – Total $35,000. PCs and peripherals (including touch screen overlays) to be used for testing and setting up a polling place mock-up. Three DRE or optical scan systems from different manufacturers.

– *Rental Facilities* – Total $18,200. Office for SRC staff and graduate students. (Total of $6,000.) Office for Dechert for 12 months (at $600 per month) for $7,200 and "polling place," probably in a mall for five months for experiments and evaluations by the general public, $5000 (at $1,000 per month).

– *Conference* – Total $10,000. The conference will be held in Sacramento and it will be designed for one day and lunch will be served. The costs would be for food, organization, renting a space, etc. All county and state election officials will be invited as well as people from the state legislature. Hence, it could run to 100 people or more.

TOTAL COSTS: The total direct cost for completing these steps is $426,000. In addition, there will be a University fee for indirect costs that will run anywhere from 10% to 36% of the project cost. All or part of this can be waived under some circumstances.

Privacy Issues in an Electronic Voting Machine

Arthur M. Keller, UC Santa Cruz and Open Voting Consortium
ark@soe.ucsc.edu
David Mertz, Gnosis Software, Inc.
mertz@gnosis.cx
Joseph Lorenzo Hall, UC Berkeley
School of Information Management and Systems
jhall@sims.berkeley.edu
Arnold Urken, Stevens Institute of Technology
aurken@stevens.edu

1. Introduction – Why a secret ballot?

The requirements for secrecy in elections depend upon the values and goals of the political culture where voting takes place. Gradations of partial and complete privacy can be found in different cultural settings. For instance, in some cantons in Switzerland, voters traditionally communicate their choices orally in front of panel of election officials.[1] In contrast, in most modern polities, the ideal of complete privacy is institutionalized by relying on anonymous balloting.[2]

The use of secret balloting in elections—where a ballot's contents are disconnected from the identity of the voter—can be traced back to the earliest use of ballots themselves. The public policy rationales for instituting anonymous balloting are typically to minimize bribery and intimidation of the voter. For example, in Athens, Greece during the sixth century B.C.E., Athenians voted by raising their hands "except on the question of exiling someone considered dangerous to the state, in which case a secret vote was taken on clay ballots."[3] In this case, presumably it was deemed necessary to vote via secret ballot to avoid bodily harm to the voter.

Secret ballots, although not always required, have been in use in America since colonial times.[4] The Australian Ballot, [5] one which is guarantees all ballots to be uniform in appearance because it is printed and distributed by the government, was adopted in throughout most of the US the late 1800's. Today, approximately one hundred years after most states in the US passed legal provisions for anonymous balloting, a strong sense of voter privacy has emerged as a third rationale. All fifty states have provisions in their constitutions for either election by "secret ballot" or elections in which "Secrecy shall be preserved," which has been interpreted by the courts as an implied requirement for secret balloting.[6] West Virginia doesn't *require* a secret ballot and leaves that to the discretion of the voter.[7] Fourteen states[8] don't list "secret" balloting or "secrecy" of elections and/or ballots and instead have either state laws (election code) or caselaw (decided legal cases in that state) that either mandate secret balloting or interpret the phrase "Election shall be by ballot" to mean a "secret ballot."

These cultural values and practices contribute to the sets of user requirements that define the expectations of voters in computer-mediated elections[9] and determine alternative sets of specifications that can be considered in developing open source software systems for elections. The Open Voting Consortium (OVC)[10] has developed a model election system that aims as one of its goals to meet these requirements. This paper describes how the OVC model ensures ballot privacy.

The OVC has developed the model for an electronic voting system largely in response to the reliability, usability, security, trustworthiness, and accessibility concerns of other voting systems. Privacy was kept in mind throughout the process of designing this system. Section 2 of this paper discusses the requirements for a secret ballot in more detail. Section 3 considers how secrecy could be compromised in some systems. Section 4 describes the architecture of the polling place components of the OVC system. Section 5 describes how the OVC handles the privacy concerns. Conclusion, acknowledgements, and references follow. While this paper focuses mostly on privacy issues for US-based elections, and how they are addressed in the OVC system, many of the issues raised are applicable elsewhere.

2. Secret Ballot Requirements

The public policy goals of secret balloting[11]—to protect the privacy of the elector and minimize undue intimidation and influence—are supported by federal election laws and regulations. The Help America Vote Act of 2002[12] codifies this as "anonymity" and "independence" of all voters, "privacy" and "confidentiality" of ballots and requires that the Federal Election Commission create standards that "[preserve] the privacy of the voter and the confidentiality of the ballot."[13]

The Federal Election Commission (FEC) has issued a set of Voting System Standards (VSS)[14] that serve as a model of functional requirements that elections systems must meet before they can be certified for use in an election. The FEC VSS state explicitly:

> To facilitate casting a ballot, all systems shall: [...] Protect the secrecy of the vote such that the system cannot reveal any information about how a particular voter voted, except as otherwise required by individual State law;[15]

and:

> All systems shall provide voting booths [that shall] provide privacy for the voter, and be designed in such a way as to prevent observation of the ballot by any person other than the voter;[16]

as well as a lengthy list of requirements that Direct Recording Electronic (DRE) voting systems must specifically meet.[17] The first basic, high level requirement of not exposing any information about how an individual voted is required of all voting systems before certification and is the most important. The second requirement listed above is a corollary.

It is not sufficient for electronic voting systems to merely anonymize the voting process from the perspective of the voting machine. Every time a ballot is cast, the voting system adds an entry to one or more software or firmware logs that consists of a timestamp and indication that a ballot was cast. If the timestamp log is combined with the contents of the ballot, this information becomes much more sensitive. For example, it can be combined with information about the order of votes cast collected at the polling place with overt or covert surveillance equipment—from cell phone cameras to security cameras common at public schools—to compromise the confidentiality of the ballot. As described below, system information collected by the voting system should be kept separated from the content of cast ballots and only used in conjunction by authorized, informed elections officials.

3. How Secrecy Could Be Compromised

3.1 A voter's secret identity

When a voter enters a polling place, she enters with a valuable secret: her identity. A secret ballot is not really "secret" in a general sense—it is possible, and even required for certain recipients, to disclose ballots—but only in the sense that it is blind as to the identity of the voter who cast it. The anonymity of ballots must apply even to most statistical properties of the voters who cast them; a notable exception, however, is in the disclosure of the geographic residence of voters who vote certain ways in the aggregate. We all know there are "Republican precincts" and "Democratic precincts," and anyone can easily and legally find out which are which.

Complicating matters is the fact that a voter's secret, her identity, *must* be disclosed at a certain stage in the voting process. To be allowed to vote at all, a voter must authenticate her right to

vote using her identity, if only by a declaration of purported identity to elections workers. Depending on jurisdiction, different standards of identity authentication apply—some require identification cards and/or revelation of personal information outside the public domain—but in all cases, identity acts as a kind of key for entry to voting. However, this key must legally be removed from all subsequent communication steps in the voting process.

The act of voting, and the acts of aggregating those votes at subsequently higher levels (called "canvassing" in voting parlance) can be thought of as a series of information channels. At a first step, a voter is given a token to allow her vote to pass through later stages; depending on the system model, this token may be a pre-printed ballot form, a PIN-style code, a temporary ballot-type marker, an electronic smart card, or at a minimum simply permission to proceed. Although the OVC has not yet decided which token is used to enable to voter to proceed, we will focus on smart cards in this paper, because they have the most serious implications for privacy. Outside the US, tokens such as hand stamps in indelible ink are also used, particularly to preclude duplicate votes being cast.

Once at a voting station, a voter must perform some actions using either pen-and-paper, a mechanical device like a lever machine or a punch card guide, or an electronic interface, such as a touchscreen or headphones-with-keypad. After performing the required voting actions, some sort of record of the voter's selections is created, either on paper, in the state of gears, or on electronic/magnetic storage media (or some combination of those). That record of selections becomes the "cast ballot." Under the Open Voting Consortium system, the paper ballot produced at a voting station undergoes final voter inspection before being *cast* into a physical ballot box.

After votes are cast, they are canvassed at several levels: first precinct; then county, district, or city; then perhaps statewide. At each level of canvassing, either the literal initial vote records or some representation or aggregation of them must be transmitted.

3.2 Understanding covert channels

At every stage of information transmission, from voter entry, through vote casting, through canvassing, a voter's identity must remain hidden. It is relatively simple to describe the overt communication channels in terms of the information that actually *should* be transmitted at each stage. But within the actual transmission mechanism it is possible that a *covert* channel also transmits improper identity information.

Covert channels in a voting system can take a number of forms. Some covert channels require the cooperation of collaborators, either voters themselves or poll workers. Other covert channels can result from (accidental) poor design in the communication channels; still others covert channels can be created by malicious code that takes advantage of incomplete channel specification. A final type of covert channel is what we might call a "sideband attack"—that is, there may be methods of transmitting improper information that are not encoded directly in the overt channel, but result indirectly from actual implementations.

For illustrations, let us briefly suggest examples of several types of covert channels. One rather straightforward attack on voter ballot anonymity is repeatedly missed by almost every new developer approaching design from a databases-and-log-files background. If the voting channels contain information about the times when particular ballots are cast and/or the sequence of ballots, this information can be correlated with an under-protected record of the sequence of times when voters enter a polling place. We sometimes call this a "covert videotape" attack. In

part, this attack uses a sideband: the covert videotaping of voters as they enter; but it also relies on a design flaw in which ballots themselves are timestamped, perhaps out of a goal to aid debugging.

A pure sideband attack is using Tempest equipment[18] to monitor the EM emissions of voting stations (if electronic ones are used). In principle, it might be possible for an attacker to sit across the street from a polling place with a van full of electronics, watch each voter enter, then detect each vote she selects on a touchscreen voting station.

Cooperative attacks require the voter or poll worker to do something special to disclose identity. As with other attacks, these covert channels need not rely on electronics and computers. For example, a malicious poll worker might mark a pre-printed blank paper ballot using ultraviolet ink before handing it to a targeted voter. The covert channel is revealed only with an UV lamp, something voters are unlikely to carry to inspect ballots. A voter herself might cooperate in a covert channel in order to facilitate vote buying or under threat of vote coercion. One such covert channel is to instruct a bought or coerced voter to cast "marked votes" to prove she cast the votes desired by her collaborator. Unique write-in names and unusual patterns in ranked preference or judicial confirmations are ways to "mark" a ballot as belonging to a particular voter.

3.3 Links Between Registration Data and Ballots

Since the voter must identify herself when signing in at the polling place, there is the potential for her identity to be tied to her vote. The token given to the voter to allow her to vote may contain her identity. For example, the voter's registration number could be entered into the smart-card writer and then encoded on the smart card that is given to the voter to enable use of a Direct Recording Electronic voting machine. When the voter registration list is given to the polling place on paper, this channel appears less of an issue. However, if voter registration list is handled electronically, then the smart card could easily contain the voter's identity. Diebold's stated intent makes this issue a potentially serious privacy risk.

> Diebold already has purchased Data Information Management Systems, one of two firms that have a dominant role in managing voter-registration lists in California and other states.
>
> "The long-term goal here is to introduce a seamless voting solution, all the way from voter registration to (vote) tabulation," said Tom Swidarski, Diebold senior vice president for strategic development.[19]

4. OVC System Overview

The Open Voting Consortium (OVC) is developing a PC-based open source voting machine with an accessible voter-verified paper ballot. The polling place system consists of a Voter Sign-in Station, an Electronic Voting Machine, an Electronic Voting Machine with a Reading Impaired Interface, a Ballot Verification Station, and a Ballot Reconciliation Station. In addition, there are components at the county canvassing site that are discussed only briefly in this paper.

4.1 Voter Sign-in Station

The Voter Sign-In Station is used by the poll worker when the voter signs in and involves giving the voter a "token." It is a requirement that each voter cast only one vote and that the vote cast be of the right precinct and party for the voter. The "token" authorizes the voter to cast a ballot using one of these techniques.

- Pre-printed ballot stock
    - Option for scanning ballot type by EVM
- Poll worker activation
- Per-voter PIN (including party/precinct identifier)
- Per-party/precinct token
- Smart cards

The token is then used by the Electronic Voting Machine and the Electronic Voting Machine with the Reading Impaired Interface to ensure that each voter votes only once and only using the correct ballot type.

If the voter spoils a ballot, the ballot is marked spoiled and kept for reconciliation at the Ballot Reconciliation Station, and the voter is given a new token for voting.

4.2 Electronic Voting Machine

The Electronic Voting Machine consists of these components:

- A PC, preferably stock commodity hardware, with these features:
    - A monitor, preferably LCD, possibly 17" touch-screen measured diagonally.
    - One or more input devices, such as:
        - Touch-screen interface on LCD screen
        - Mouse
        - Keyboard
        - Buttons surrounding the screen, like on an ATM
        - Numeric keypad
        - Symbolic keypad
    - Possibly a smart card reader/writer
- A CD-R drive. The CD-R will contain:
    - The operating system, e.g., a stripped down Linux distribution
    - The EVM software
    - Ballot Definition files and public keys of various external components
    - Optionally, sound files for the ballot (included for the Electronic Voting Machine with the Reading Impaired Interface)
    - Personalization, potentially including public/private key pairs for this voting machine
    - Startup record, possibly including generated public key of this voting machine
    - Electronic Ballot Images (EBIs), in XML format (and possibly in Postscript format), written at end of day in ascending order by (randomly generated) ballot ID
    - The CD-R is used subsequently by the Ballot Reconciliation System and possibly during county canvassing.
- A printer with these specifications:
    - Inkjet or laser
    - Preferably output page is obscured from view (either by appearing face down, or by a cover)
    - Unprintable margin of no more than 7.5mm on all sides
    - Feedback to the user (auditory or visual) that the ballot is printing and will come out soon
    - Prints a test document at the start of a voting day that includes records of the

public keys for the EVM for this day.
    - Potentially takes blank ballot stock given to voter upon sign-in. Otherwise, includes storage for blank ballot stock for printing. Blank ballot stock may be specially printed paper, possibly pre-printed on reverse side (with "please turn over" message).
    - Prints ballot in printed ballot format potentially using special printed ballot stock.
    - The ballot can be read by the Ballot Verification Station and includes text in OCR format, plus a barcode for more foolproof reading.
- A persistent EBI storage device, such as a USB memory dongle (i.e., a USB flash memory device) for persistently storing the EBIs until the end of the day, when the EBIs are transferred onto the CD-R. The USB memory dongle is kept for audit purposes.
    - Device should be large enough not to be easily lost
    - Device should be lockable and tamper proof when locked
    - Potentially, device could lock in the open position onto cabinet and PC and lock in the closed position sealed and ready for removal. Device could be set to be open only once, and on subsequent openings the device would be read only.
    - Potentially, with hardware private key for digitally signing the ballot.
- Security enclosure that prevents tinkering with the device

4.3 Electronic Voting Machine with Reading Impaired Interface

The Electronic Voting Machine with Reading Impaired Interface is a PC similar to the Electronic Voting Machine described above that includes auditory output of the ballot choices and selections made and also includes additional modes of making selections suitable for the blind or reading impaired. Whether these features are integrated to a common voting machine with all functionality, or whether there is a separate configuration for the disabled, is an open question. For example, additional modes of input may be useful for those who can read printed materials, but have physical limitations. The idea is for a universal design that accommodates all voters.

The electronic voting machine for the reading impaired produces a printed ballot that can be processed by the Ballot Verification Station.

4.4 Ballot Verification Station

The Ballot Verification Station reads the ballot produced by the Electronic Voting Machine or the Electronic Voting Machine with Reading Impaired Interface and speaks (auditorily) the selections on the voter's ballot. A count is kept of usage, including counts of consecutive usage for the same ballot, but no permanent record is kept of which ballots are verified.

The PC boots off the CD-R, which includes the following:

- The operating system
- The BVS software
- Ballot Definition files and public keys of various Electronic Voting Machines
- Sound files for the ballot
- Personalization
- Startup record
- Non-ballot identifying statistics on usage

It is possible for the Ballot Verification Station to have a screen and to display the selections on the screen at the voter's option. Such an option (enabled by the voter upon her request) would enable a voter who can read to verify that her ballot will be read correctly for automated tallying.

4.5 Ballot Reconciliation Station

The Ballot Reconciliation Station reads the paper ballots and reconciles them against the Electronic Ballot Images (EBIs) on the CD-Rs from the Electronic Voting Machine or the Electronic Voting Machine with Reading Impaired Interface.

The Ballot Reconciliation Station includes the following components:

- Scanner, preferably page fed
- PC
- Monitor
- Input devices: keyboard, mouse
- Printer
    - Prints vote totals for posting
- CD-R
    - Like the other CD-R; includes cumulative copy of EBIs as well as vote totals by precinct.

The Ballot Reconciliation System runs the Ballot Reconciliation Procedure, which is beyond the scope of this paper.

4.6 Paper Ballot

The paper ballot is generated by the Electronic Voting Machine or the Electronic Voting Machine with Reading Impaired Interface. It is the paper on which the voter's choices are recorded. It must be "cast" in order to be tallied during canvassing, testing, or a manual recount.

The paper ballot is intended to be easily read by the voter so that the voter may verify that his or her choices have been properly marked. It also contains security markings and a bar code. The bar code encodes the user's choices, as expressed in the human readable portion of the ballot. The human readable text should be in an OCR-friendly font so it is computer-readable as well. The voter may use the Ballot Verification Station to verify that the bar code accurately reflects their choices. The Ballot Verification Station not only assists sight-impaired and reading-impaired voters in verifying their ballots, but also to give any voter the assurance that the bar-code on the ballot properly mirrors their choices, as represented in the human-readable text on the ballot.

The bar code consists of several things:

- Identifiers, such as the date, election, precinct, type of ballot, polling machine, and random ballot ID for reconciliation against the electronic record made by the Electronic Voting Machine or the Electronic Voting Machine with Reading Impaired Interface.
- The selections made by the voter.
- Checksums to detect processing errors.
- Additional padding data to obscure the bar code so that poll workers, who will be able to see the bar code (but not the textual part of the ballot) will not be readily able to ascertain by eye what selections the voter made.
- The bar code is designed so that none of the information in the bar code can be used to identify any voter personally.

Spoiled paper ballots are kept by the Ballot Reconciliation System to be reconciled against Electronic Ballot Images (EBIs) produced by the Electronic Voting Machine or the Electronic Voting Machine with Reading Impaired Interface.

4.7 Privacy Folder

The paper ballot contains the voter's choices in two forms: a form that can be read by people and a bar code that expresses those choices in a machine readable form.

Poll workers may come in contact with the ballot should they be asked to assist a voter or to cast the ballot into the ballot box. In order to protect voter privacy it is desirable to minimize the chance that a voting place worker might observe the voter's ballot choices.

A privacy folder is just a standard file folder with an edge trimmed back so that it reveals only the bar code part of a ballot. The voter is expected to take his/her ballot from the printer of the Electronic Voting Machine or the Electronic Voting Machine with Reading Impaired Interface and place it into a privacy folder before leaving the voting booth.

The privacy folder is designed so that the voter may place the ballot still in its folder against the scanning station of Ballot Verification Station to hear the voter's ballot's choices spoken.

When handed the ballot by the voter, the poll worker casts the ballot by turning the privacy folder so the ballot is face down, and then sliding the paper ballot into the ballot box.

4.8 Ballot Box

This is a physically secure container, into which voters have their paper ballots placed, in order to "cast" their votes. The mechanical aspects of the voting box will vary from jurisdiction to jurisdiction, depending on local laws and customs.

4.9 Box for Spoiled Ballots

When a voter spoils a ballot, perhaps because the ballot does not accurately reflect her preferences, the ballot is marked spoiled and placed in a box for spoiled ballots for later reconciliation.

5. OVC Balances Security, Reliability and Privacy

This section discusses how the Open Voting Consortium (OVC) is balancing security, reliability and privacy in its electronic voting system.

5.1 The (circumscribed) advantage of Free and Open Source Software

Opening the source code to a voting system—all stages of it, not only the voting station—is a necessary, though not sufficient, condition for insuring covert channels are eliminated, or at least curtailed. For practical purposes, no system that functions as a black box, in which the implementing source code is maintained as a trade secret, can be known to lack covert channels. Any channel with non-optimal utilization includes non-utilized content that is potentially malicious rather than merely accidental—behavior analysis, in principle, cannot distinguish this difference.

Of course, free and open source code is not sufficient to prevent covert channels. Sideband channels, in particular, are never exposed by direct examination of source code in isolation; it is necessary here to perform additional threat modeling. But even direct encoding of extra

information *within* an overt channel can sometimes be masked by subtle programming tricks. More eyes always reduce the risk of tricks hidden in code. Parallel implementation to open specifications, and message canonicalization also helps restrict channels to overt content.

A frequent criticism of free and open source software is that, while the code is available for inspection, no coordinated inspection is actually conducted.[20] The absence of Non-Disclosure Agreements and restrictive intellectual property agreements makes it possible for the large body of open source developers to inspect the code. Furthermore, in the realm of elections systems—that are mission-critical for a democratic government—open source software could benefit from a specific group of developers who are tasked with recognizing and repairing vulnerabilities. This is a common need in many open source software projects, and in this sense, it might be an appropriate role for a non-profit institution that delivered such services to other important projects like GNU/Linux, BIND, the Mozilla tool suite and the Apache web server.

5.2 Randomization of ballot-IDs

Under the OVC design ballots carry ballot-IDs. In our prototype, these IDs are four digit numbers, which provides enough space for ten thousand ballots to be cast at a polling place. We anticipate this ballot-ID length to remain sufficient in production. The main purpose of ballot-IDs is simply to enable auditing of official paper ballots against unofficial electronic ballot images.

The crucial feature of ballot-IDs is that they must not reveal any information about the sequence of votes cast. The prototype and current reference implementation use Python's 'random' module to randomize the order of ballot-IDs. The module uses the well-tested Mersenne Twister algorithm, with a periodicity of $2^{19937}-1$. Seeding the algorithm with a good source of truly random data—such as the first few bytes of /dev/random on modern Linux systems—prevents playback attacks to duplicate ballot-ID sequences.

Because the ballot-IDs are generated at random by each of the electronic voting machines, it is important that two machines do not use the same random ballot-ID. As a result, the first digit (or character) of the ballot-ID in the reference platform will represent the voting machine ID for that polling place.

The remaining 3 digits of the ballot-ID are randomly selected from the range of 000 to 999. A list is maintained of already used ballot-IDs for this electronic voting machine for this election. (One way to obtain such a list is to scan the stored EBIs for the ballot numbers used.) If the random number generated matches an already used ballot-ID, then that number is skipped and a new random number is generated.

5.3 Privacy issues with barcodes

The Open Voting Consortium system design uses a barcode to automate the scanning of paper ballots. Such barcodes raise several possibilities for introducing covert channels.

The prototype/demo system presented by OVC, for example, used a 1-D barcode, specifically Code128. For vote encoding, selections were first converted to a decimal number in a reasonably, but not optimally, efficient manner; specifically, under the encoding particular digit positions have a direct relationship to corresponding vote selections. These digits, in turn, are encoded using the decimal symbology mode of Code128.

Coauthor Mertz identified the problem that even though barcodes are not per-se human readable, identical patterns in barcodes, especially near their start and end positions, could be recognized by observers. This recognition would likely even be unconscious after poll workers saw hundred of exposed barcodes during a day. For example, perhaps after a while, a poll worker notices that known Bush supporters always have three narrow bars followed by a wide bar at the left of their barcode, while known Kerry supporters have two wide bars and two narrow bars. To prevent this attack, 1-D barcodes undergo a simple obfuscation of rotating digits by amounts keyed to a repetition of the random ballot-id. This "keying" is not even weak encryption—it resembles a Caeser cipher,[21] but with a known key; it is just a way to make the same vote not look the same on different ballots.

In the future, OVC anticipates needing to use 2-D barcodes to accommodate the information space of complex ballots and ancillary anonymity-preserving information such as globally unique ballot-IDs and cryptographic signatures. At this point, we anticipate that patterns in 2-D barcodes will not be vulnerable to visual recognition; if they are, the same kind of obfuscation used already is straightforward. But the greatly expanded information space of 2-D barcodes is a vulnerability as well as a benefit. More bit space quite simply makes room to encode more improper information. For example, if a given style of barcode encodes 2000 bits of information, and a particular ballot requires 500 bits to encode, those unused 1500 bits can potentially contain improper information about the voter who cast the ballot.

Just because a barcode has *room* for anonymity-compromising information does not mean that information is actually encoded there, of course. Preventing misuse of an available channel requires orthogonal steps. Moreover, even a narrow pipe can disclose quite a lot; it only takes about 10 bits to encode a specific address within a precinct using a lookup table. Even a relatively impoverished channel might well fit a malicious ten bits. For example, if a non-optimal vote encoding is used to represent votes, it is quite possible that multiple bit-patterns will correspond to the same votes if strictly defined canonicalization is not used. The choice among "equivalent" bit patterns might leak information.

Eliminating barcodes, it should be noted, does not necessarily eliminate covert channels in a paper ballot. It might, however, increase voter confidence as average voters become less *concerned* about covert channels (which is both good and bad). For example, even a barcode-free printed ballot could use steganography[22] to encode information in the micro-spacing between words, or within security watermarks on the page.

5.4 Privacy in the Voting Token (e.g., Smart Card)

As observed above, the token given to the voter to enable her to use the electronic voting machine might contain information that could compromise anonymity. Indeed, it is not possible to demonstrate the absence of covert channels through black box testing. Analysis of the software is important to show how the data for the smart card is assembled. Above, we considered the benefits of open source software in that numerous people, both inside and outside the process, have the ability to inspect and test the software to reduce the likelihood of covert channels remaining. Furthermore, the smart-card enabling hardware includes an interface used by the poll worker (the Voter Sign-In Station). The nature of that interface limits the type of information that can be encoded. Encoding the time of day in the smart card, either intentionally or as a side effect of the process of writing files to the smart card, is a potential avenue for attack.

However, the electronic voting machine receiving the smart card knows the time as well, so the smart card is not needed to convey this information.

We propose to encode in the voting token the ballot type and (particularly for multiple precincts at the same polling place) the precinct. The smart card should also be digitally signed by the smart card enabling hardware, so as to help reduce forgeries.

5.5 Information Hidden in Electronic Ballot Images and Their Files

The electronic ballot images (EBIs) are stored on the electronic voting machine where the ballot was created. One purpose of maintaining these EBIs is to reconcile them against the paper ballots, to help preclude paper ballot stuffing. The EBIs are in XML format, which can be interpreted when printed in "raw" form.

We prefer not to store the EBIs in a database on the electronic voting machine. A database management system incurs additional complexity, potential for error, and can contain sequence information that can be used to identify voters. On the other hand, flat files in XML format would include the date and time in the file directory, and that is also a potential privacy risk. We can mitigate this risk by periodically 'touch'ing EBI files during voting station operation, in order to update the date and time of all files to the latest time. The placement order of the files on the disk however may still disclose the order of balloting.

Another approach is to store all the EBIs in a single file as if it were an array. Suppose that it is determined that the largest XML-format EBI is 10K bytes. Since there are 1000 possible ballot-IDs for this electronic voting machine, it is possible to create a file with 1000 slots, each of which is 10K in length. When the ballot is to be printed, the random ballot-ID is chosen, and the EBI is placed in that slot in the file, padded to the full 10K in length with spaces (which would be removed during canonicalization). The file can be updated in place, thereby having only the latest date and time. Alternatively, two files can be used, and the electronic voting machine writes to one, waits for completion, and then writes to the other. The benefit of this approach is increased reliability of persistent storage of the EBI file.

A similar technique can be used to maintain copies of the Postscript versions of the ballots.

At the close of polling place, the electronic voting machine is changed to close out the day's voting. At this time, the EBIs are written as individual flat files in ascending ballot-ID order to a new session of the CD-R that already contains the electronic voting machine software and personalization. Because the EBIs are written all at once, and in order by ascending random ballot-ID, anonymity is preserved.

5.6 Reading Impaired Interface

The reading impaired interface is used by both voters who cannot read and voters who cannot see. Having a segregated electronic voting machine used only by the reading and visually impaired can compromise privacy. It is therefore desirable for the electronic voting machines with the reading impaired interface to be used also by those who can read. For example, if all electronic voting machines incorporated the reading impaired interface, then those voters would not be segregated onto a subset of the voting machines.

It is important that the ballot not record the fact that a particular ballot was produced using the reading impaired interface. Nor should the electronic voting machine maintain such information

in a way that identifies specific ballots. If a separate reading impaired voting station is used, the ballot-ID should be generated in a manner that does not identify the voting station used.

Nonetheless, it is useful for the electronic voting machine to maintain some statistics on the use of the reading impaired interface, provided that these statistics cannot identify specific ballots or voters. These statistics could be used to improve the user interface, for example.

5.7 Printed Ballot

The printed ballot contains a human readable version of the voter's selections. After all, that is how it is a voter-verifiable paper ballot. However, the secrecy of the voter's selections is at risk while the voter carries the paper ballot from the electronic voting machine, optionally to the ballot validation station, and on to the poll worker to cast her ballot.

Our approach is to use a privacy folder to contain the ballot. When the voter signs in, she receives the token plus an empty privacy folder. When the electronic voting machine prints the ballot, the voter takes the ballot and places it in the privacy folder, so that only the barcode shows. The barcode can be scanned by the ballot validation station without exposing the human readable portion of the ballot. When the privacy folder containing the ballot is given to the poll worker to be cast, the poll worker turns the privacy folder so the ballot is face down and then slides the ballot out of the privacy folder and into the official ballot box. The poll worker thus does not see the text of the ballot, with the possible exception of precinct and (for primaries) party identifiers that may be printed in the margin.

The privacy folder is an ordinary manila folder trimmed along the long edge so that the barcode sticks out.

5.8 Ballot validation station

The ballot validation station allows visually impaired voters—anyone—to hear and therefore validate their paper ballots. A blind voter can carry a paper ballot in a privacy folder and be assured that the ballot is still private. Since only the barcode of the ballot (and possibly the ballot type—the precinct and party for primaries) is viewable (and as mentioned above, the barcode is obscured), it is best to keep the paper ballot in the privacy folder. So the ballot validation station should be able to read the barcode without removing the paper ballot from the privacy folder. The back of the ballot should have a barcode (possibly preprinted) saying "please turn over," so a ballot validation station will know to tell the blind voter that the ballot is upside down. So that others will not hear the ballot validation station speak the choices on the ballot, the voter will hear these choices through headphones.

It may be useful to know how many times the ballot validation station was used, and how many consecutive times the same ballot is spoken. It is important to assure that the ballot-IDs are not persistently stored by the ballot validation station. In particular, to tell how many consecutive times the same ballot was spoken, the ballot validation station must store the previous ballot-ID. However, once another ballot with a different ballot-ID is read, then that the new ballot-ID replaces the previous ballot-ID. And the ballot-ID field should be cleared at end of day closeout. The counts of consecutive reads of the same ballot should be a vector of counts, and no other ordering information should be maintained. Inspection of the code together with clear interfaces of the records persistently maintained can help assure privacy.

5.9 Languages

Steve Chessin identified a problem with ballots for non-English speakers. For the voter, the ballot must be printed in her own language. However, for canvassing and manual counts, the ballot and its choices must also be printed in English. However, this approach makes bilingual ballots easy to identify, and that can compromise ballot anonymity if only a small number of voters in a given precinct choose a particular language. Steve Chessin's solution is to have all ballots contain both English and another language, where the other language is randomly chosen for English speakers.[23]

It is important to make the Ballot Validation Station handle multiple languages. This requirement implies that the voter can choose the language for validating the ballot. To simply this process, the ballot barcode can include a notation of the second language, but only if that information does not compromise anonymity. Always choosing a second language at random, reduces the risk. When the ballot's barcode is scanned by the Ballot Validation Station, the voter is given a choice of these two languages for the spoken choices listed on the ballot.

5.10 Public Vote Tallying

It is important that the ballots be shuffled before publicly visible scanning occurs using the Ballot Reconciliation System. The ballots will naturally be ordered based on the time they were placed in the ballot box. As described above, the time or sequence of voting is a potential risk for privacy violations.

An illustration of this problem was reported privately to coauthor Keller about a supposedly secret tenure vote at a university. Each professor wrote the decision to grant or deny tenure on a piece of paper. The pieces of paper were collected and placed on top of the pile one-by-one in the sequence by where the person was sitting. The pile was then turned over and the votes were then read off in the ballots in the reverse of that sequence as they were tallied. One observer noted how each of the faculty members voted in this supposedly secret vote.

5.11 Results by Precinct

A key approach to ensuring the integrity of county (or other district) canvassing (i.e., vote tallying) is to canvass the votes at the precinct and post the vote totals by contest at the precinct before sending on the data to the county. As a cross-check, the county should make available the vote totals by contest for each precinct. However, because the county totals include absentee votes, it is difficult to reconcile the posted numbers at the precinct against the county's totals by precinct, unless the county separates out absentee votes (plus hand-done polling place votes). However providing these separations may reduce the aggregation size to impair anonymity. Even worse is when provisional ballots are incrementally approved and added to the tally one-by-one.

We propose to exclude provisional ballots from the results posted at the precinct. The county tallies by precinct should be separated by those votes included in the precinct-posted tally and those votes not included in the precinct-posted tally. As long as there is a publicly viewable canvassing of the votes not included in the precinct-posted tally, then trust is better addressed. If that canvassing process involves ballots separated from the envelope containing the voter's identity, then privacy is enhanced.

The totals by precinct are aggregate counts for each candidate. There is no correlation among specific ballots, an important factor to help assure privacy. However, Ranked Preference Voting

schemes, such as Instant Runoff Voting, require that the ordering of the candidates must be separately maintained for each ballot. Vote totals are useful to help assure that each vote was counted, but they do not contain enough information to produce an absolute majority winner. Therefore, vote totals can be posted at the precinct, independent of ranking, and those totals can also be posted at the county. A voter who specifies a write-in candidate for a Ranked Preference Voting race may be doing so as a marker for observation during the canvassing process. To reinstate anonymity, write-in candidates whose vote totals are below a certain threshold could be eliminated from the canvassing process. This threshold must be set to avoid distortions of aggregate scores at the county level.

5.12 Privacy in the face of voter collusion

Complex cast ballots, taken as a whole, inevitably contain potential covert channels. We reach a hard limit in the elimination of improper identifying information once voter collusion is considered. In an ideal case, voters cooperate in the protection of their own anonymity; but threats of vote coercion or vote buying can lead voters to collaborate in disclosing—or rather, proving—their own identity. It is, of course, the right of every voter to disclose her own votes to whomever she likes; but such disclosure must not be subject to independent verifications that attack voter anonymity as a whole.

Elections with many contests, with write-ins allowed, or with information-rich ranked preference contests, implicitly contain extra fields in which to encode voter identity. For example, if an election contains eight judicial retention questions, there are at least 6561 possible ways to complete a ballot, assuming Yes, No, and No Preference are all options for each question. Very few precincts will have over 6561 votes cast within them, so a systematic vote buyer could demand that every voter cast a uniquely identifying vote pattern on judicial retentions. That unique pattern, plus the precinct marked on a ballot, in turn, could be correlated with a desired vote for a contested office.

Ballots may not generally be completely separated into records by each individual contest. For recounts or other legal challenges to elections, it is generally necessary to preserve full original ballots, complete with correlated votes. Of course it is physically possible to cut apart the contest regions on a paper ballot, or to perform a similar separation of contests within an EBI. However, doing so is not generally permissible legally.

The best we can do is control the disclosure of full ballots to mandated authorities, and with maintenance of chain-of-custody over ballots, including of EBIs. A full ballot must be maintained, but only aggregations of votes, per contest, are disclosed to the general public; the number of people who have access to full ballots should be as limited as feasible, and even people with access to some full ballots should not necessarily be granted general access to all full ballots.

5.13 Privacy in Electronic Voting Machines with Voter-Verifiable Paper Audit Trails

This section discusses other approaches to a voter-verifiable paper audit trails. These issues do *not* apply to the design described in this paper of the voter-verifiable paper *ballot.*[24]

Rebecca Mercuri has proposed that Direct Recording Electronic (DRE) voting machines have a paper audit trail that is maintained under glass, so the voter does not have the opportunity to touch it or change it.[25] Some vendors are proposing that paper from a spool be shown to the voter, and if the ballot is verified a cutter releases the paper audit trail piece to drop into the box

for safekeeping. [26] The challenge with this approach is to make sure that all of the paper audit trail is readable by the voter, doesn't curl away out of view, and yet the paper audit trails from previous voters is obscured from view. Furthermore, there is the problem that the paper audit trail falls in a more-or-less chronologically ordered pile. Furthermore, the problem of reconciling the paper audit trail with the electronic ballot image is difficult to do in an automated manner if the paper audit trail cannot be sheetfed.

Another approach is to keep the paper audit trail on a continuous spool.[27] While this approach has the potential to be more easily scanned in an automated fashion for reconciliation, privacy is compromised by maintaining an audit trail of the ballots cast in chronological order. We described above why maintaining order information is a problem for privacy.

6. Conclusion

We have described the Open Voting Consortium's voting system that includes a PC-based open-source voting machine with a voter-verifiable accessible paper ballot, and discussed the privacy issues inherent in this system. By extension, many of the privacy issues in this paper also apply to other electronic voting machines, such as DREs (Direct Recording Electronic voting machines). The privacy issues illustrate why careful and thorough design is required for voter privacy. Imagine how much work is required to ensure that such systems are secure and reliable.

7. Acknowledgements

We acknowledge the work of the volunteers of the Open Voting Consortium who contributed to the design and implementation we describe. In particular, Alan Dechert developed much of the design and Doug Jones provided significant insights into voting issues. The demonstration software was largely developed by Jan Kärrman, John-Paul Gignac, Anand Pillai, Eron Lloyd, David Mertz, Laird Popkin, and Fred McLain. Karl Auerbach wrote an FAQ on which the OVC system description is based. Amy Pearl also contributed to the system description. Kurt Hyde and David Jefferson gave valuable feedback. David Dill referred some of the volunteers.

8. References

[1] Benjamin Barber, Strong Democracy, Twentieth Anniversary Edition, University of California Press, 2004.
[2] Alvin Rabushka and Kenneth Shepsle, Politics in Plural Societies: A Theory of Democratic Instability. Columbus: Merrill, 1972.
[3] See page 9 of: Albright, Spencer, *The American Ballot*, American Council on Public Affairs, Washington, D.C., 1942.
[4] In 1682, the Province of Pennsylvania in its Frame of the Government required "THAT all the elections of Members or Representatives of the People, to serve in the Provincial Council and General Assembly ... shall be resolved and determined by ballot. (Votes and Proceedings of the House of Representatives of the Province of Pennsylvania. Printed and sold by B. Franklin and D. Hall, at The New Printing Office, near the Market. Philadelphia, Pennsylvania MDCCLII, Page xxxi.)

In 1782, the legislature of the Colony/State of New Jersey tried to intimidate Tories by requiring viva voce voting. (At that time, about half of New Jersey voted with ballots and the other half viva voce.) They rescinded this in their next session. (The History of Voting in New Jersey, Richard P. McCormick, Rutgers University Press, Brunswick, New Jersey, 1953, Page 74). In 1796, the State of New Jersey required federal elections to be by ballot and extended that to state elections the following year. (Ibid, Page 106.)

In the 1853 pamphlet SECRET SUFFRAGE, Edward L. Pierce recounted Massachusetts' battle to make the secret ballot truly secret. The Massachusetts Constitution in 1820 required elections for representatives to have "written" votes. In 1839, the legislature attacked the secrecy of the written ballot by requiring the ballot to be presented for deposit in the ballot box open and unfolded. In 1851, the legislature passed the "Act for the better security of the Ballot," which provided that the ballots are to be deposited in the ballot box in sealed envelopes of uniform size and appearance furnished by the secretary of the Commonwealth (State of Massachusetts). The battle waged until a provision in the State Constitution made the secret ballot mandatory. (SECRET SUFFRAGE, Edward L. Pierce, Published by the Ballot Society, No. 140 Strand, London, England 1853, Page 7.)

[5] The more general "Australian ballot" is a term used for anonymous balloting using official non-partisan ballots distributed by the government. See Albright 1942 at 26. "The very notion of exercising coercion and improper influence absolutely died out of the country." Albright, 1942 at 24 quoting Francis S. Dutton of South Australia in J. H. Wigmore's *The Australian Ballot System* (2nd ed.), Boston, 1889, 15-23.
[6] For example, The Delaware Supreme Court recognized that the Delaware's constitutional language amounts to an "implied constitutional requirement of a secret ballot." *Brennan v. Black* 34 Del. Ch. 380 at 402. (1954)
[7] "In all elections by the people, the mode of voting shall be by ballot; but the voter shall be left free to vote by either open, sealed or secret ballot, as he may elect." (W. Va. Const. Art. IV, § 2 (2003))
[8] Maryland, Minnesota, Mississippi, Nevada, New Hampshire, New Jersey, North Carolina, Ohio, Oaklahoma, Oregon, Rhode Island, Tennessee, Texas and Vermont.

[9] Arnold B. Urken, Voting in a Computer-Networked Environment, in Carol Gould (ed.) The Information Web: Ethical and Social Implications of Computer Networking, Boulder: Westview Press, 1989.
[10] The Open Voting Consortium (OVC) is a non-profit organization dedicated to the development, maintenance, and delivery of open voting systems for use in public elections. See http://www.openvotingconsortium.org/
[11] There are two aspects to anonymous voting. The first is ballot privacy—the ability for someone to vote without having to disclose their vote to the public. The second is secrecy—someone should not be able to prove that they voted one way or another. The desire for the latter is rooted in eliminating intimidation while the former is to curb vote-buying. The history of these two concepts is beyond the scope of this paper.
[12] The Help America Vote Act of 2002 (HAVA), 42 U.S.C.A. §§ 15301 - 15545 (West 2004).
[13] *Id.*, § 301(a)(1)(C). (Also see §§ 242(a)(2)(B), 245(a)(2)(C), 261(b)(1), 271(b)(1), 281 (b)(1), 301(a)(3)(A))
[14] Federal Election Commission, Voting System Standards, Vols. 1 & 2 (2002), available at http://www.fec.gov/pages/vssfinal/ (Microsoft DOC format) or http://sims.berkeley.edu/~jhall/fec_vss_2002_pdf/ (Adobe PDF format).
[15] *Id.*, at Vol. 1, § 2.4.3.1(b).
[16] *Id.*, at Vol. 1, § 3.2.4.1.
[17] *Id.*, at Vol. 1, § 3.2.4.3.2(a)-(e) (hardware) and § 4.5 (software).
[18] http://cryptome.org/nsa-tempest.htm
[19] Ian Hoffman, "With e-voting, Diebold treads where IBM wouldn't," Oakland Tribute, Sunday, May 30, 2004, http://www.oaklandtribune.com/Stories/0,1413,82~1865~2182212,00.html
[20] Fred Cohen, *Is Open Source More or Less Secure?*, Managing Network Security, July 2002.
[21] http://www.fact-index.com/c/ca/caesar_cipher.html
[22] Neil F. Johnson and Sushil Jajodia, "Steganography: Seeing the Unseen," *IEEE Computer*, February 1998: 26-34.
[23] It is important to note that the procedure for randomizing the second, non-English language printed on a ballot would have to be quite good. Flaws in the randomization or maliciously planted code could result in the "marking" of certain ballots leading to a compromise of ballot privacy. A simple solution would be to have all ballots printed only in English, and requiring non-English literate voters to use the BVA to verify their vote auditorily. As an alternative for ballots printed only in English, ballot overlays could by provided for each language needed for each ballot type. The overlay could either be in heavy stock paper printed with the contest names with holes for the selections to show through, or it could be a translation sheet showing all the contest names and selections translated into non-English language. In the former case, the ballots would have to be have the layout of each contest fixed, so it would be necessary to have extra spaces when the length of the results vary, such as for pick up to 3 candidates when only 2 were selected. These overlays could be tethered to every voting machine so that voters who read only a specific language could simply place the overlay over their ballot so that she could read their selections as if the ballot was printed in their native language. The overlay approach reduces confusion for English speakers and it also reduces the length of the printed ballot.
[24] See http://evm2003.sourceforge.net/security.html for the difference between a paper receipt and a paper ballot, and between a paper audit trail and an electronically generated paper ballot.
[25] Rebecca Mercuri, "A Better Ballot Box?," *IEEE Spectrum Online*, October 2002,

http://www.spectrum.ieee.org/WEBONLY/publicfeature/oct02/evot.html
[26] Avante VOTE-TRAKKER™ EVC308,
http://www.aitechnology.com/votetrakker2/evc308.html
[27] Sequoia Voting Systems, "Sequoia Voting Systems Announces Plan to Market Optional Voter Verifiable Paper Record Printers for Touch Screens in 2004,"
http://www.sequoiavote.com/article.php?id=54

A PC-Based Open-Source Voting Machine with an Accessible Voter-Verifiable Paper Ballot

Arthur M. Keller, UC Santa Cruz and Open Voting Consortium
ark@soe.ucsc.edu
Alan Dechert, Open Voting Consortium
alan@openvotingconsortium.org
Karl Auerbach, InterWorking Labs
karl@iwl.com
David Mertz, Gnosis Software, Inc.
mertz@gnosis.cx

1. Introduction

The heart of democracy is voting. The heart of voting is trust that each vote is recorded and tallied with accuracy and impartiality.

The Open Voting Consortium (OVC) is creating a trustworthy, cost effective, voter verifiable voting system using open source software components on industry standard computers. A primary element of this Open Voting system is the use of software through which the voter creates a printed paper ballot containing his or her choices. Before casting his or her ballot the voter may use other, independently programmed, computers to validate that the ballot properly reflects the voter's choices. The paper ballot is cast by placing it into a ballot box. Once cast, that paper ballot is the authoritative record of the voter's choices for the election and for any recount of that election. Open Voting ballots are machine-readable and may be tabulated (and verified and re-tabulated in the case of a recount) either by computer or by hand.

Open Voting systems can be engineered to accommodate the special needs of those who have physical impairments, or limited reading ability.

Voting is the foundation of democratic systems, whether those be direct or representative systems. There is no shortage of historical anecdotes of attempts to undermine the integrity of electoral systems. The paper and mechanical systems we use today, although far from perfect, are built upon literally hundreds of years of actual experience.

There is immense pressure to replace our "dated" paper and mechanical systems with computerized systems. There are many reasons why such systems are attractive. These reasons include, cost, speed of voting and tabulation, elimination of ambiguity from things like "hanging chads", and a belated recognition that many of our traditional systems are not well-suited for use by citizens with physical impairments.

Many of us today have come to trust many of our financial transactions to ATM's (automatic teller machines). The push for electronic voting machines has been a beneficiary of that faith in ATMs. However, we are starting to learn that that faith is unwarranted.

First of all, ATM machines do fail and are often attacked. Those who operate ATM's usually consider the loss rate to be a proprietary secret. Banks are well versed in the actuarial arts and

they build into their financial plans various means to cover the losses that do occur. In more crude terms, it's only money.

Voting machines carry a more precious burden - there is no way to buy insurance or to set aside a contingency fund to replace a broken or tampered election.

There are several areas of concern regarding the new generation of computerized voting machines:

- No means for the voter to verify that his/her votes have been tallied properly.
- No means outside of the memories of the voting machines themselves to audit or recount the votes.
- Lack of ability to audit the quality of the software. Fortunately the widespread belief that "computers are always right" is fading. Our individual experiences with error-ridden software on personal computers and consumer products (e.g. the BMW 745i[1]), software errors by even the best-of-the-best (e.g. NASA and the loss of the Mars Climate Orbiter[2]), and the possibility that intentional software bugs can be hidden so deeply as to be virtually invisible (Ken Thompson's famous 1984 paper - Reflections on Trusting Trust[3]) have all combined to teach us that we should not trust software until that trust has been well earned. And even then, we ought not to be surprised if unsuspected flaws arise.
- Vulnerability of the machines or of their supporting infrastructures to intentional attack or inadvertent errors.

The companies that produce voting machines have poured gasoline onto the smoldering embers of concern. Some of these products are built on Microsoft operating systems - operating systems that have a well-earned reputation for being penetrable and insecure. And most of these companies claim that their systems are full of trade secrets and proprietary information and that, as a consequence, their internal workings may not be inspected by the public. In addition, these companies have frequently displayed a degree of disdain (in some cases disdain that takes the form of lawsuits) against those who are concerned about the integrity of these products. And finally, these companies themselves have frequently demonstrated an appalling lack of sophistication regarding the protection of their systems, procedures, and corporate computer systems. There is a widespread perception that these companies are more concerned about profits than about fair and trustworthy elections.

The Help America Vote Act of 2002[4] was passed into law to modernize voting equipment as a result of the 2000 US Presidential election and the problems observed in Florida.[5] The Federal Election Commission (FEC) has issued a set of Voting System Standards (VSS)[6] that serve as a model of functional requirements that elections systems must meet before they can be certified for use in an election. The next section discusses the existing voting machines that meet those standards. Section 3 considers the rationale for an accessible voter-verifiable paper ballot. Section 4 is a description of the Open Voting Consortium architecture for the polling place. Section 5 mentions the current state and next steps. Conclusion, acknowledgements, and references follow.

2. Existing Electronic Voting Machines

Existing DRE (Direct Recording Electronic) voting machines have come under increasing scrutiny.

2.1 Diebold AccuVote TS and TS-X

A group led by Avi Rubin analyzed the Diebold AccuVote TS DRE voting machine and found numerous flaws.[7] SAIC was commissions by the state of Maryland to do another analysis of the Diebold voting system and found "[t]he system, as implemented in policy, procedure, and technology, is at high risk of compromise."[8] Based on these reports, the California Secretary of States office established security procedures for DRE voting machines.[9] Diebold used uncertified software in their electronic voting equipment in California.[10] Diebold was then banned from California elections by the California Secretary of State.[11]

2.2 Other DRE Voting Machines

Other DRE vendors are proposing to add printers to their DREs.[12] AccuPoll has an Electronic Voting System with a voter-verified paper audit trail.[13] Sequoia Voting Systems is marketing optional voter verifiable paper record printers for their DREs.[14] The state of Nevada will use these VeriVote printers in the 2004 election.[15] The Avante VOTE-TRAKKER is a DRE with a voter-verifiable paper audit trail.[16]

3. Why an Accessible Voter-Verifiable Paper Ballot

Many computer and other experts have joined VerifiedVoting.org's call for "the use of voter-verified paper ballots (VVPBs) for all elections in the United States, so voters can inspect individual permanent records of their ballots before they are cast and so meaningful recounts may be conducted. We also insist that electronic voting equipment and software be open to public scrutiny and that random, surprise recounts be conducted on a regular basis to audit election equipment."[17]

3.1 Paper Receipts vs. Paper Ballots

We speak of OVC creating a paper *ballot*, not a receipt, nor simply a "paper trail." That is, for OVC machines, the printout from a voting station is the primary and official record of votes cast by a voter. Electronic records may be used for generating preliminary results more rapidly, but the paper ballot is the actual official vote document counted.

Some writers discuss producing a paper receipt, which a voter might carry home with them, as they do an ATM receipt. There are two significant problems with this approach. In the first place, if we suppose that a voting station might have been tampered with and/or simply contain a programming error, it is not a great jump to imagine that it may print out a record that differs from what it records electronically. A receipt is a "feel good" approach that fails to correct the underlying flaws of DREs.

But the second problem with receipts is even more fundamental. A voting receipt that can be carried away by a voter enables vote buying and vote coercion. An interested third party—even someone as seemingly innocuous as an overbearing family member—could demand to see a receipt for voting in a manner desired. With OVC systems, ballots must be placed into a sealed ballot box to count as votes. If a voter leaves with an uncast ballot, even if she went through the motions of printing it at a vote station, that simply does not represent a vote that may be "proven" to a third party.

What some vendors refer to as a paper trail suffers from a weakness similar to the first problem paper receipts suffer. Under some such models, a DRE voting station might print out a summary of votes cast at the end of the day (or at some other interval). But such a printout is also just a "feel good" measure. If a machine software or hardware can be flawed out of malice or error, it can very well print a tally that fails to accurately reflect the votes cast on it. It is not *paper* that is crucial, but *voter-verifiability*.

3.2 Paper Audit Trail Under Glass vs. Paper Ballot.

While "ballot under glass" does indeed do a pretty good job of preventing ballot box stuffing with forged physical ballots, this approach is not the only—nor even the best—technique to accomplish this goal. We plan for OVC systems to incorporate cryptographic signatures and precinct-level customization of ballots that can convincingly prove a ballot is produced on authorized machines, at the voting place, rather than forged elsewhere. A simple customization of ballots is a variation of the page position of our ballot watermarks in a manner that a tamperer cannot produce in advance. Surprisingly much information can be subtly coded by moving two background images a few millimeters in various directions. Another option is to encode a cryptographic signature within the barcode on a ballot—in a manner that can be mathematically proven not to disclose anything about the individual voter who cast that vote, but simultaneously that cannot be forged without knowledge of a secret key.

There are several narrowly technical problems with "ballot under glass" systems. For one thing, such a system will almost inevitably be more expensive than one that can use commodity printers and paper stock, such as OVC's solution. But voting is too important to be decided on cost, so that is an incidental issue. Along a similar line, a "ballot under glass" system has some extra mechanical problems with allowing rejection of incorrect ballots; some sort of mechanism for sending a spoiled ballot somewhere other than to the ballot-box is needed. Again, this adds cost and more points of physical failure.

A more significant issue for "ballot under glass" systems is their failure to provide the quality of accessibility to vision- or reading-impaired voters that OVC's design does. Ordinary sighted voters who happen to need reading glasses are likely to find "ballot under glass" systems more difficult to check than are OVC printed ballots. Even if these machines add provisions for audio feedback on final ballots, users are dependent on the very same machine to provide such audio feedback. Potentially, a tampered-with machine could bias votes, but only for blind voters (still perhaps enough to change close elections). In contrast, OVC positively encourages third parties to develop software to assure the barcode encoding of votes matches the visibly printed votes—every voter is treated equally, and all can verify ballots.

From a more sophisticated cryptology perspective, "ballot under glass" systems are likely to compromise voter anonymity in subtle ways. One of the issues the world-class security researchers with OVC have considered is the possibility that sequential or time-stamp information on ballots could be correlated with the activity of individual voters. Even covert videotaping of the order in which voters enter a polling place might be used for such a compromise. This is just part of the threat analysis study that we plan to perform in order to create a reliable, secure, and trustworthy election system.

3.3 Accessible Voting

One of the key benefits of Electronic Voting Machines is to allow disabled voters to vote unassisted. [18] However, as the movement for a voter-verifiable paper audit trail grows,[19] there is a need for the paper audit trail to be accessible as well.[20] The Open Voting Consortium's voting system is designed to be accessible for both entering the votes and verifying the paper ballot produced.

4. OVC System Overview

The Open Voting Consortium (OVC) is developing a PC-based open source voting machine with an accessible voter-verified paper ballot. The polling place system consists of a Voter Sign-in Station, an Electronic Voting Machine, an Electronic Voting Machine with a Reading Impaired Interface, a Ballot Verification Station, and a Ballot Reconciliation Station. In addition, there are components at the county canvassing site that are discussed only briefly in this paper.

4.1 Voter Sign-in Station

The Voter Sign-In Station is used by the poll worker when the voter signs in and involves giving the voter a "token." It is a requirement that each voter cast only one vote and that the vote cast be of the right precinct and party for the voter. The "token" authorizes the voter to cast a ballot using one of these techniques.

- Pre-printed ballot stock
    - Option for scanning ballot type by EVM
- Poll worker activation
- Per-voter PIN (including party/precinct identifier)
- Per-party/precinct token
- Smart cards

The token is then used by the Electronic Voting Machine and the Electronic Voting Machine with the Reading Impaired Interface to ensure that each voter votes only once and only using the correct ballot type.

If the voter spoils a ballot, the ballot is marked spoiled and kept for reconciliation at the Ballot Reconciliation Station, and the voter is given a new token for voting.

4.2 Electronic Voting Machine

The Electronic Voting Machine consists of these components:

- A PC, preferably stock commodity hardware, with these features:
    - A monitor, preferably LCD, possibly 17" touch-screen measured diagonally.
    - One or more input devices, such as:
        - Touch-screen interface on LCD screen
        - Mouse
        - Keyboard
        - Buttons surrounding the screen, like on an ATM
        - Numeric keypad
        - Symbolic keypad
    - Possibly a smart card reader/writer
- A CD-R drive. The CD-R will contain:

    - The operating system, e.g., a stripped down Linux distribution
    - The EVM software
    - Ballot Definition files and public keys of various external components
    - Optionally, sound files for the ballot (included for the Electronic Voting Machine with the Reading Impaired Interface)
    - Personalization, potentially including public/private key pairs for this voting machine
    - Startup record, possibly including generated public key of this voting machine
    - Electronic Ballot Images (EBIs), in XML format (and possibly in Postscript format), written at end of day in ascending order by (randomly generated) ballot ID
    - The CD-R is used subsequently by the Ballot Reconciliation System and possibly during county canvassing.
- A printer with these specifications:
    - Inkjet or laser
    - Preferably output page is obscured from view (either by appearing face down, or by a cover)
    - Unprintable margin of no more than 7.5mm on all sides
    - Feedback to the user (auditory or visual) that the ballot is printing and will come out soon
    - Prints a test document at the start of a voting day that includes records of the public keys for the EVM for this day.
    - Potentially takes blank ballot stock given to voter upon sign-in. Otherwise, includes storage for blank ballot stock for printing. Blank ballot stock may be specially printed paper, possibly pre-printed on reverse side (with "please turn over" message).
    - Prints ballot in printed ballot format potentially using special printed ballot stock.
    - The ballot can be read by the Ballot Verification Station and includes text in OCR format, plus a barcode for more foolproof reading.
- A persistent EBI storage device, such as a USB memory dongle (i.e., a USB flash memory device) for persistently storing the EBIs until the end of the day, when the EBIs are transferred onto the CD-R. The USB memory dongle is kept for audit purposes.
    - Device should be large enough not to be easily lost
    - Device should be lockable and tamper proof when locked
    - Potentially, device could lock in the open position onto cabinet and PC and lock in the closed position sealed and ready for removal. Device could be set to be open only once, and on subsequent openings the device would be read only.
    - Potentially, with hardware private key for digitally signing the ballot.
- Security enclosure that prevents tinkering with the device

4.3 Electronic Voting Machine with Reading Impaired Interface

The Electronic Voting Machine with Reading Impaired Interface is a PC similar to the Electronic Voting Machine described above that includes auditory output of the ballot choices and selections made and also includes additional modes of making selections suitable for the blind or reading impaired. Whether these features are integrated to a common voting machine with all functionality, or whether there is a separate configuration for the disabled, is an open question.

For example, additional modes of input may be useful for those who can read printed materials, but have physical limitations. The idea is for a universal design that accommodates all voters.

The electronic voting machine for the reading impaired produces a printed ballot that can be processed by the Ballot Verification Station.

4.4 Ballot Verification Station

The Ballot Verification Station reads the ballot produced by the Electronic Voting Machine or the Electronic Voting Machine with Reading Impaired Interface and speaks (auditorily) the selections on the voter's ballot. A count is kept of usage, including counts of consecutive usage for the same ballot, but no permanent record is kept of which ballots are verified.

The PC boots off the CD-R, which includes the following:

- The operating system
- The BVS software
- Ballot Definition files and public keys of various Electronic Voting Machines
- Sound files for the ballot
- Personalization
- Startup record
- Non-ballot identifying statistics on usage

It is possible for the Ballot Verification Station to have a screen and to display the selections on the screen at the voter's option. Such an option (enabled by the voter upon her request) would enable a voter who can read to verify that her ballot will be read correctly for automated tallying.

4.5 Ballot Reconciliation Station

The Ballot Reconciliation Station reads the paper ballots and reconciles them against the Electronic Ballot Images (EBIs) on the CD-Rs from the Electronic Voting Machine or the Electronic Voting Machine with Reading Impaired Interface.

The Ballot Reconciliation Station includes the following components:

- Scanner, preferably page fed
- PC
- Monitor
- Input devices: keyboard, mouse
- Printer
    - Prints vote totals for posting
- CD-R
    - Like the other CD-R; includes cumulative copy of EBIs as well as vote totals by precinct.

The Ballot Reconciliation System runs the Ballot Reconciliation Procedure, which is beyond the scope of this paper.

4.6 Paper Ballot

The paper ballot is generated by the Electronic Voting Machine or the Electronic Voting Machine with Reading Impaired Interface. It is the paper on which the voter's choices are recorded. It must be "cast" in order to be tallied during canvassing, testing, or a manual recount.

The paper ballot is intended to be easily read by the voter so that the voter may verify that his or her choices have been properly marked. It also contains security markings and a bar code. The bar code encodes the user's choices, as expressed in the human readable portion of the ballot. The human readable text should be in an OCR-friendly font so it is computer-readable as well. The voter may use the Ballot Verification Station to verify that the bar code accurately reflects their choices. The Ballot Verification Station not only assists sight-impaired and reading-impaired voters in verifying their ballots, but also to give any voter the assurance that the bar-code on the ballot properly mirrors their choices, as represented in the human-readable text on the ballot.

The bar code consists of several things:

- Identifiers, such as the date, election, precinct, type of ballot, polling machine, and random ballot ID for reconciliation against the electronic record made by the Electronic Voting Machine or the Electronic Voting Machine with Reading Impaired Interface.
- The selections made by the voter.
- Checksums to detect processing errors.
- Additional padding data to obscure the bar code so that poll workers, who will be able to see the bar code (but not the textual part of the ballot) will not be readily able to ascertain by eye what selections the voter made.
- The bar code is designed so that none of the information in the bar code can be used to identify any voter personally.

Spoiled paper ballots are kept by the Ballot Reconciliation System to be reconciled against Electronic Ballot Images (EBIs) produced by the Electronic Voting Machine or the Electronic Voting Machine with Reading Impaired Interface.

4.7 Privacy Folder

The paper ballot contains the voter's choices in two forms: a form that can be read by people and a bar code that expresses those choices in a machine readable form.

Poll workers may come in contact with the ballot should they be asked to assist a voter or to cast the ballot into the ballot box. In order to protect voter privacy it is desirable to minimize the chance that a voting place worker might observe the voter's ballot choices.

A privacy folder is just a standard file folder with an edge trimmed back so that it reveals only the bar code part of a ballot. The voter is expected to take his/her ballot from the printer of the Electronic Voting Machine or the Electronic Voting Machine with Reading Impaired Interface and place it into a privacy folder before leaving the voting booth.

The privacy folder is designed so that the voter may place the ballot still in its folder against the scanning station of Ballot Verification Station to hear the voter's ballot's choices spoken.

When handed the ballot by the voter, the poll worker casts the ballot by turning the privacy folder so the ballot is face down, and then sliding the paper ballot into the ballot box.

4.8 Ballot Box

This is a physically secure container, into which voters have their paper ballots placed, in order to "cast" their votes. The mechanical aspects of the voting box will vary from jurisdiction to jurisdiction, depending on local laws and customs.

4.9 Box for Spoiled Ballots

When a voter spoils a ballot, perhaps because the ballot does not accurately reflect her preferences, the ballot is marked spoiled and placed in a box for spoiled ballots for later reconciliation.

5. Current Status and Next Steps

A demonstration system was shown at the Santa Clara County Government Building in San Jose, California on April 1, 2004. This demonstration was featured on KGO-TV and KCBS and KGO radio later that day and described in the San Jose Mercury News that morning.[21] On April 8, 2004, the San Jose Mercury News referred to our system in an editorial as a "Touch Screen Holy Grail."[22] Further demonstrations were given at the Computers, Freedom, and Privacy conference in Berkeley, California on April 23, 2004.[23] Another demonstration was given at the PlaNetwork conference in San Francisco, California on June 6, 2004.[24]

Several state colleges and the Open Voting Consortium are currently in discussions with their respective Secretaries of States to obtain HAVA funding to build production-quality reference versions of this system.

6. Conclusions

The Open Voting Consortium has demonstrated a voting system based on a PC-based electronic voting machine with voter-verifiable accessible paper ballot. We have described the design for the production system we propose to build, based on the prototype we have built and the lessons learned in the process. In the development of this system, we expect to enhance the state of the art in building reliable and trustworthy computerized systems. However, it is not merely the software and hardware components that are of concern; the voting processes and procedures are also key to the development of a reliable, secure, trustworthy and accessible system.

7. Acknowledgements.

We acknowledge the efforts of the volunteers of the Open Voting Consortium who contributed to the design we describe. In particular, Alan Dechert developed much of the design and Doug Jones provided significant insights into voting issues. The demonstration software was largely developed by Jan Kärrman, John-Paul Gignac, Anand Pillai, Eron Lloyd, David Mertz, Laird Popkin, and Fred McLain. Karl Auerbach wrote an FAQ on which parts of this paper is based. Amy Pearl also contributed to the system description. Joseph Lorenzo Hall contributed useful background.

Our work was inspired by Curtis Gans, Roy Saltman, Henry Brady, Ronnie Dugger, Irwin Mann, and others who have spoken out on the need for auditable, consistent, secure and open election administration. In the last two years, David Dill and Bev Harris have been especially helpful. David Dill referred several people to the OVC, and he and Bev Harris have helped the public recognize the need for a voter-verified paper audit trail.

8. References.

[1] Dorian Miller, "BMW 745 Bug," September 22, 2002, found at http://www.cs.unc.edu/~dorianm/academics/comp290test/bmw745bug.html

[2] Greg Clark, Staff Writer and Alex Canizares, "Navigation Team Was Unfamiliar with Mars Climate Orbiter," posted November 10, 1999, found at http://www.space.com/news/mco_report-b_991110.html

[3] Ken Thompson, "Reflections on Trusting Trust," *Communication of the ACM*, Vol. 27, No. 8, August 1984, pp. 761-763, found online at http://www.acm.org/classics/sep95/.

[4] The Help America Vote Act of 2002 (HAVA). 42 U.S.C.A. §§ 15301 - 15545 (West 2004). See http://fecweb1.fec.gov/hava/hava.htm

[5] Lorrie Faith Cranor, "Voting After Florida: No Easy Answers," March 19, 2001, available from http://lorrie.cranor.org/voting/essay.html

[6] Federal Election Commission, Voting System Standards, Vols. 1 & 2 (2002), available at http://www.fec.gov/pages/vssfinal/ (Microsoft DOC format) or http://sims.berkeley.edu/~jhall/fec_vss_2002_pdf/ (Adobe PDF format).

[7] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, *Analysis of an Electronic Voting System*, Proc. IEEE Symposium on Security and Privacy (May, 2004), found at http://avirubin.com/vote/analysis/index.html

[8] http://www.dbm.maryland.gov/dbm_search/technology/toc_voting_system_report/votingsystemreportfinal.pdf

[9] See http://www.ss.ca.gov/elections/ks_dre_papers/ks_ts_press_release.pdf

[10] See http://www.wired.com/news/evote/0,2645,61637,00.html?tw=wn_tophead_2

[11] See http://www.ss.ca.gov/executive/press_releases/2004/04_030.pdf

[12] See http://www.wired.com/news/business/0,1367,58738,00.html

[13] See http://www.accupoll.com/News/PressReleases/2003-10-10.html

[14] See http://www.sequoiavote.com/mediadetail.php?id=74

[15] See http://www.wired.com/news/evote/0,2645,63618-2,00.html?tw=wn_story_page_next1

[16] See http://www.aitechnology.com/votetrakker2/evc308.html

[17] See http://www.verifiedvoting.org/

[18] See http://www.accessiblesociety.org/topics/voting/electionreformlegis.html

[19] See http://www.verifiedvoting.org/

[20] See http://www.ss.ca.gov/elections/ks_dre_papers/avvpat_standards_6_15_04.pdf and http://www.ss.ca.gov/elections/ks_dre_papers/press_release_avvpat_06_15_04.pdf

[21] See http://www.siliconvalley.com/mld/siliconvalley/8328014.htm

[22] See http://www.kentucky.com/mld/mercurynews/news/opinion/8383100.htm

[23] See http://cfp2004.org/program/#votingmachinedemo

[24] See http://www.planetwork.net/2004conf/program.html

Analysis of an Electronic Voting System

IEEE Symposium on Security and Privacy, Oakland, CA, May, 2004.

Authors

Tadayoshi Kohno
Adam Stubblefield
Aviel D. Rubin
Dan S. Wallach

Abstract

With significant U.S. federal funds now available to replace outdated punch-card and mechanical voting systems, municipalities and states throughout the U.S. are adopting paperless electronic voting systems from a number of different vendors. We present a security analysis of the source code to one such machine used in a significant share of the market. Our analysis shows that this voting system is far below even the most minimal security standards applicable in other contexts. We identify several problems including unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor software development processes. We show that voters, without any insider privileges, can cast unlimited votes without being detected by any mechanisms within the voting terminal software. Furthermore, we show that even the most serious of our outsider attacks could have been discovered and executed without access to the source code. In the face of such attacks, the usual worries about insider threats are not the only concerns; outsiders can do the damage. That said, we demonstrate that the insider threat is also quite considerable, showing that not only can an insider, such as a poll worker, modify the votes, but that insiders can also violate voter privacy and match votes with the voters who cast them. We concludethat this voting system is unsuitable for use in a general election. Any paperless electronic voting system might suffer similar flaws, despite any "certification" it could have otherwise received. We suggest that the best solutions are voting systems having a "voter-verifiable audit trail," where a computerized voting system might print a paper ballot that can be read and verified by the voter.

Paper: PDF

Rebuttal

On July 30, 2003, Diebold posted a "technical analysis" of our report at http://www2.diebold.com/checksandbalances.pdf.

Our response is available at: http://avirubin.com/vote/response.html.

Doug Jones from the University of Iowa Department of Computer Science also responded to their analysis http://www.cs.uiowa.edu/~jones/voting/dieboldftp.html#rebuttals.

SAIC Report

In early August 2003 the state of Maryland hired a third-party consulting firm (SAIC) to perform an analysis of Diebold's AccuVote-TS voting system. On September 24, 2003, Maryland made SAIC's report public. To quote the SAIC report, "[t]he system, as implemented in policy, procedure, and technology, is at high risk of compromise." Despite the problems identified in our report and in the SAIC report, Maryland is still planning to proceed with the 55.6 million dollar purchase of Diebold AccuVote-TS voting terminals.

To help mitigate the risks identified in the security analyses, Maryland proposed a set of technological changes to Diebold's voting machines as well as procedural changes to the election process. While this may help "raise the bar," it is impossible to know whether any security analysis identifies all the possible vulnerabilities present in an analyzed system. By only patching the known vulnerabilities, Maryland is not actually ensuring that the voting system will be secure. Rather, Maryland should follow security engineering best practices, which state that security can only be assured through a rigorous design process that considers security from a project's conception, not through a set of patches applied after the fact.

It appears that the state of Maryland has had to compromise on the security of the voting system due to the election calendar. The Maryland State Board of Elections states that "an alternative system could not be implemented in time to conduct the March 2004 Presidential Primary election and could jeopardize the November 2004 Presidential General election." Unfortunately, by compromising on security, the integrity and privacy of these elections may still be in jeopardy.

RABA Report

The consulting firm, RABA, has issued a report on the security of the Diebold machines. They validated our findings and found other problems as well. Perhaps the best coverage of this study is in a Wired report by Kim Zetter.

Questions for vendors

We have compiled a list of questions you can ask your vendors for people considering buying voting machines.

Testimony, U.S. Election Assistance Commission

Dr. Aviel D. Rubin, Professor of Computer Science
May 5, 2004

My name is Avi Rubin. I am a Professor of Computer Science and Technical Director of the Information Security Institute at Johns Hopkins University. I am author or co-author of several widely used books on the subject of computer and network security, and I have chaired several of the top security research conferences. I received my Ph.D. in Computer Science from the University of Michigan in 1994 in the specialization of Computer Security. I have been researching security issues related to electronic voting since 1997. Last year, by invitation of the Department of Defense, I served on the security peer review group of the SERVE voting system for absentee voting for military personnel and overseas civilians. I also participated as a panelist in the 2000 National Science Foundation study of the feasibility of electronic voting. Last year, my research team analyzed the code used in the Diebold Accuvote TS and TSx and wrote a report citing many security flaws that we found. Our study was published in the top peer reviewed computer security conference, the IEEE Symposium on Security and Privacy. I am a member of the National Committee on Voting Ingerity, and in March, I served as an election judge in Baltimore County where Diebold Accuvote TSx machines were used.

I am here as an expert in a particular domain, namely computer security. I recognize that voting is a complicated issue with a diverse set of values, each of which is very important to the functioning of this process in a way that is reliable and trustworthy in the broadest sense. Security is a necessary component of a fair and accurate election process. However, there are other equally important components. Making sure that everyone can participate in a way that is private and independent is also key to our electoral process. Making sure that people from all walks of life, regardless of how recently they arrived in this country, can participate in the process in a language they can comprehend is also important. An accurate and secure system that limits the ability of individuals with disabilities and language minorities would fall short of meeting the goals of our democracy, as would a system that allowed everyone to participate but failed to protect the integrity and accuracy of their vote. Luckily, security and accessibility are not competing goals. While today's DREs increase accessibility, they do not provide adequate security. Appropriately designed voting systems, can provide accessibility and security. Our commitment to a fair, inclusive, secure election process requires us to demand both from our election machinery.

I come before you today to contribute my expertise garnered over years of experience as one of the leading computer security experts in my field. You will hear from experts representing the disability community and the civil rights community. They are experts in their domains. In my domain, I speak with authority. Given that we all agree that security is an important component of elections, I ask that you hear me and understand the serious nature of my critique of current DREs.

My primary concerns with today's DREs are:

- There is no way for voters to verify that their votes were recorded correctly.
- There is no way to publicly count the votes.
- In the case of a controversial election, meaningful recounts are impossible.

- The machines must be completely trusted. They must be trusted not to fail, not to have been programmed maliciously, and not to have been tampered with at any point prior to or during the election. We have techniques for building secure systems, and they are not being utilized.
- With respect to the Diebold Accuvote TS and TSx, we found gross design and programming errors, as outlined in our attached report. The current certification process resulted in these machines being approved for use and being used in elections.
- We do not know if the machines from other vendors are as bad as the Diebold ones because they have not made their systems available for analysis.

Since our study came out, three other major studies often referred to as the SAIC report, the Ohio reports, and the RABA report, all cited serious security vulnerabilities in DREs. RABA, which is closely allied with the National Security Agency, called for a "pervasive rewrite" of Diebold's code. Yet, the vendors, and many election officials, such as those in Maryland and Georgia continue to insist that the machines are perfectly secure. I cannot fathom the basis for their claims. I do not know of a single computer security expert who would testify that these machines are secure. I personally know dozens of computer security experts who would testify that they are not.

I have been disappointed that the policy community did not reach out to the computer security community when making decisions about voting technology, and when my community came to the table, they said it was too late. At first I was puzzled by the lack of attention to the security critiques of DREs. Today I am outraged. At this point the failures of current DREs have been documented in four major studies by leading computer security experts, and we have ample field experience documenting failures at the polling place. Yet computer security experts, myself included, find ourselves routinely referred to as luddites and conspiracy theorists. Failing to confer with computer security experts in decisions about voting technology was a mistake. Given the gravity of the security failings the computer security community has documented in current DRE systems it is irresponsible to move forward without addressing them.

Addressing the problems I and others have documented with DREs requires more than just fixing the machines. We must reform the process for establishing voting technology to provide transparency. Vendors are not subject to public code review. In the one instance where independent security experts had an opportunity to examine a voting system, the results proved that the current process results in machines being deployed with unacceptable lack of quality control. We cannot achieve perfectly secure systems; such things do not exist. But on the spectrum of terrible to very good, we are sitting at terrible. Not only have the vendors not implemented security safeguards that are possible, they have not even correctly implemented the ones that are easy.

If I had more time (and I would be happy to address such issues in the Q & A) I would debunk the myth of the security of the so-called triple redundancy in the Diebold machines. I would explain the limitations of logic and accuracy testing in an adversarial setting, I would explain how easy it would be for a malicious programmer to rig the election with today's DREs, and I would describe the seriousness of the security flaws that we and others have found in the Diebold machines. These are all things that I could have done and would have been happy to do, before anybody started purchasing and using these DREs. But nobody asked.

I'd like to stress one important point. Security and functionality are completely different things. Functionality is whether or not something works when it is used as planned. Functionality can be

tested, and the tests can be used to make predictions about the future behavior of a system. Security, on the other hand, has to do with how a system behaves under unanticipated circumstances with an active, dynamic adversary trying to subvert it. By definition, you cannot test a system for security the way you test for functionality. It is inappropriate and incorrect to draw conclusions about the security of a system based on its past performance. The fact that this argument is consistently put forward in defense of the security of the DREs demonstrates just how much real security expertise is needed in this process. You would not design a heart implant without feedback from cardiologists. You would not design defense systems for the physical security of this country without consulting military experts, and you should not design systems for computerized elections in this country without consulting computer security experts. I can assure you from my analysis of the Diebold machines that no such expertise was utilized.

In conclusion, my colleagues and I have presented our analysis to many different groups of computer scientists, including the National Science Foundation, the National Academy of Science, and several security conferences. We have won awards for this work, and the community at large is in strong agreement with our conclusions. I recommend that the commission heed our recommendation and seek more broad input from the computer science and the computer security communities. These people have a long history of experience with designing mission critical systems. The opinions of the experts in this matter are quite different from the picture being painted by the vendors and some state officials, all of whom have much less expertise, or no expertise whatsoever, in computer security.

Speaker Biography

Dr. Aviel D. Rubin is Professor of Computer Science and Technical Director of the Information Security Institute at Johns Hopkins University. Prior to joining Johns Hopkins Rubin was a research scientist at AT&T Labs. Rubin is author of several books including Firewalls and Internet Security, second edition (with Bill Cheswick and Steve Bellovin, Addison Wesley, 2003), White-Hat Security Arsenal (Addison Wesley, 2001), and Web Security Sourcebook (with Dan Geer and Marcus Ranum, John Wiley & Sons, 1997). He is Associate Editor of ACM Transactions on Internet Technology, Associate Editor of IEEE Security & Privacy, and an Advisory Board member of Springer's Information Security and Cryptography Book Series. Rubin serves on the board of directors of the USENIX Association and on the DARPA Information Science and Technology Study Group. He is co-author of a report showing security flaws in a widely used electronic voting system that focused a national spotlight on the issue. Rubin also co-authored an analysis of the governments planned SERVE system for Internet voting for military and overseas civilians, which led to the cancellation of that dangerous project. In January, 2004 Baltimore Magazine name Rubin a *Baltimorean of the Year* for his work in safeguarding the integrity of our election process, and he is also the recipient of the 2004 Electronic Frontiers Foundation *Pioneer Award.* Rubin has a B.S, ('89), M.S.E ('91), and Ph.D. ('94) from the University of Michigan.

Analysis of an Electronic Voting System

Johns Hopkins Information Security Institute Technical Report TR-2003-19, July 23, 2003

Authors

Tadayoshi Kohno
Adam Stubblefield
Aviel D. Rubin
Dan S. Wallach

Paper: PDF

Response to Diebold's Technical Analysis

Diebold posted an analysis of our report at http://www2.diebold.com/checksandbalances.pdf. Throughout their document, they refer to details of our paper as "allegations," and they attempt to argue away these allegations with logic that is often contrived.

We have no personal ill-will toward Diebold as a company; our aim was to provide a technical analysis of the code that we had at our disposal. While our conclusions have upset those who stand to lose financially from these conclusions and those who are embarrassed by decisions they have made without the knowledge of the insecurity in the code, we firmly stand behind our findings.

Diebold claims that we are not very familiar with the election processes. However, we have extensive academic and industrial experience in software engineering, computer security, and cryptography, which forms the bases of our analysis. In this response, we show that Diebold's arguments often miss the point, do not address many of our most serious findings, and demonstrate a considerable lack of knowledge of the technical matter, including a misunderstanding of technical terms such as "safe language," as we describe below.

Also, Diebold criticized our network-based attacks as being unrealistic since the voting machines will not be networked in practice. The Diebold code we examined contains many different configuration options, including the use of wired or wireless networks and the use of modems. Any communication, whether wired or wireless, whether over the Internet or over private phone lines, is fair game for an analysis of what can be intercepted by an intruder. If there is no such communication, *only then* would the Diebold system be safe against such attacks. Our paper carefully stated these assumptions, while Diebold's response blurs this distinction.

Rather than respond with a 35 page point by point rebuttal and risk a continuously growing exchange, we focus on a few examples of Diebold's misinformation, and we show some examples of security problems that appeared in our report and for which there were no counter arguments in the Diebold "analysis". The primary example is Diebold's claim, which was widely cited in the press, that we ran the code on a different platform from the one that was intended. While this is true, it in no way reflects on our analysis. In fact, the main reason that we ran the code at all was to test whether or not it worked, and thus to help draw on opinion about whether or not it was production code. Our entire paper and our entire analysis were based on manual inspection of the source code. Thus, the platform on which we ran the code did not play into any of our findings, and Diebold's attempt to focus attention on that is a clear

effort to misdirect readers. Unfortunately, many reporters and election officials have latched onto this issue as though it was meaningful. We could have written the same paper without running the code, and perhaps we should have never even mentioned that we ran it, to avoid this confusion.

At the end of our response, we provide a list of questions people should ask, not only of Diebold, but of any direct recording electronic (DRE) voting system. If these systems are going to be used for our elections, they deserve the scrutiny that we, and others, can bring to them. Voting systems are one of the pillars of democracy. If they fail, democracy itself will fail with them.

Cryptography

Cryptography is an important part of good security designs. It is, however, notoriously difficult to get right. We have claimed that, in the Diebold code we examined, "cryptography, when used at all, is used incorrectly." We stand by this claim.

Throughout Diebold's response they seek to marginalize their dependence on cryptography (e.g., Diebold's responses to "allegation 1" and "allegation 8"), however the fact remains that although cryptography was used in their design, it was used incorrectly. In their response to allegation 8, Diebold states that our claims are "based on the presumption that there is a single correct means of using cryptography." This play on words disguises the real problem: While there is no single correct use of cryptography, the existence of many correct uses does not imply that the cryptography in the Diebold code is used correctly. As we have described in the full paper, and will summarize below, every use of cryptography in the Diebold code is flawed.

The first problem we address is key management. In modern security systems, key management is one of the chief design challenges present when using cryptography to protect data against eavesdroppers and intruders. Such systems need to be careful to change the keys on a regular basis and to limit the damage that can occur should any one key be compromised. Systems like SSL/TLS, used to communicate securely with e-commerce web sites, have remarkably sophisticated key management systems that have been carefully studied by researchers worldwide.

In the Diebold code we analyzed, both the keys for the smartcard and the keys used to encrypt the votes were static entries in the source code. This means that the same keys are used on every voting device. Thus, an attacker who was able to compromise a single voting device would have access to the keys for *all* other voting devices running the same software.

In Diebold's response to "allegation 28" they acknowledge the problems with a hard-coded smartcard key by claiming that "[t]his issue has since been resolved in subsequent versions of the software." They do not, however, explain *how* this issue has been resolved. Moreover, in their response to "allegation 43," they seemingly admit that the keys used to protect the votes are still static and fixed. Instead they claim that "[a]n attacker would need access to *both* the source code *and* the physical storage." This is not correct. The attacker only needs access to the physical storage as the key is also stored in the executable code.

A second set of problems has to do with the way that the Diebold code encrypts the votes and audit logs. The files that hold the votes are encrypted using the Data Encryption Standard (DES) algorithm in CBC mode. There are problems with the use of both DES and the CBC mode, as we describe below.

In their response to "allegation 44," Diebold states that "[t]here are stronger forms of compression than

DES, but the authors' implication that the keys can be recovered `in a short time' is deliberately misleading." We assume that Diebold meant to claim that there are stronger *encryption* algorithms available, as DES is not a compression algorithm. To support our "in a short time" claim we cited Cracking DES. This work describes the design and construction of a machine specifically engineered to recover DES keys. Using 1998 technology, the machine cost under $250,000 and was able recover a DES key in under 3 days. With today's computer technology such a machine could be made both significantly faster and less expensive. That Diebold considers the possibility of such a machine being used to find keys for an election machine ``incredibly unrealistic" demonstrates a misunderstanding of the threat model. It is not inconceivable that a well funded adversary such as the intelligence service of a foreign government would be interested in tampering with the results of a U.S. election. We note, however, that the DES Cracker was financed not by a government or university, but by a private individual. Of course, since the Diebold code included a static key, no cracking is required to compromise the security of the system if any one voting terminal can be stolen ahead of the election and disassembled to learn its key.

Not included among Diebold's list of allegations is our statement that the Diebold code uses DES incorrectly. On page 15, we note that "DES is being used in CBC mode which requires an initialization vector to ensure its security." We go on to show that the Diebold code does not provide the necessary initialization vectors. A detailed explanation of this problem is highly technical; we refer the interested reader to A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation. That Diebold does not attempt to refute this claim is troubling, especially given that in "allegation 8" they state that "the cryptography in the software is used as the developers intended." Though Diebold qualifies this by claiming that "additional security measures" and "future development" might be needed, such a clear error demonstrates a lack of cryptographic knowledge on the part of the developers.

Also omitted from Diebold's list of allegations is a third problem: the use of a CRC as a method of providing data integrity. It is a common misconception outside of the cryptographic community that encrypted data can not be meaningfully modified by an attacker. Unfortunately, this misconception is false. There are, however, cryptographic primitives known as Message Authentication Codes (MACs) which can detect such tampering. MACs are used in many widely publicized protocols, including the security protocols for the Internet. However, instead of using such a MAC, the Diebold code uses a non-cryptographic checksum called a CRC to detect whether a file has been tampered with. This is completely insecure as is discussed on page 15 of our paper. The use of CRCs instead of MACs has long been documented in the security literature as a very serious mistake.

This list of problems is not meant to be complete; there are other issues discussed in the paper such as the protected counter and the random number generator which we do not feel that Diebold has successfully refuted. However, we do believe that this list is sufficient to show the lack of cryptographic expertise utilized in the system's design. If, as Diebold claims, "the cryptography in the software is used as the developers intended" we have no faith that any cryptography present in future versions of the code will be used correctly.

Smartcards

Diebold's response raises some issues with respect to our smartcard-based attacks against the voting terminals. We first point out that, as we stated in our original report and as Diebold agrees in their response to "allegation 21," an adversary using a special "attack smartcard" could cast multiple votes. (An attacker could also make homebrew administrator and ender cards. For brevity, we focus our

discussion on voting multiple times.)

The first interesting technical question that this raises is: How easy would it be for an adversary to make such a special "attack smartcard?" Diebold's response suggests that making such an "attack smartcard" would be very difficult. As we stated in our original report, we believe otherwise and explain our reasoning in the following sections. The second interesting technical question is: What happens if an adversary inserts multiple votes? We treat these technical questions separately.

How to make "attack smartcards"

Let's look at this question from two perspectives. First we'll assume that the adversary knows the Diebold source code. We believe this is a reasonable assumption since, as recently exhibited, source code cannot always be kept secret. However, we will also examine this for the case where the adversary does not know the Diebold source code.

If the adversary knows the Diebold source code, then the adversary will know the protocol between the smartcard and the voting terminal. The adversary's goal in this case is to make his own smartcard that tricks the voting terminal into believing that it is a legitimate smartcard when it is really an "attack smartcard" or "homebrew smartcard." We observe that a computer-savvy adversary with a few hundred dollars could produce his own attack smartcard. The adversary doesn't have to work for Diebold or their third-party smartcard vendor. How would such an adversary go about producing such an attack smartcard? By purchasing a user-programmable smartcard (perhaps a Java Card) and a smartcard reader/writer and programming it appropriately. The adversary would know how to program the smartcard since he can deduce the protocol between the smartcard and the terminal from the source code. (See our paper for further discussions.)

Now what if the adversary didn't know the Diebold source code? As we note in our paper, by inserting a "wire-tap device" between the voting terminal and the smartcard, an adversary could learn enough about the protocol between the terminal and the smartcard to create his own smartcards for use by some conspirator later in the day. Diebold does point out that such an attack might be risky since the adversary might get caught. Of course, all it takes is one malicious poll worker/volunteer to ensure that some adversary somewhere doesn't get caught. Subsequently, that adversary could share his knowledge with others. (As an aside, Diebold makes the claim that voters must "sign in" when they vote, and thus some of the attacks we describe are "high risk." To this we remark that in many states it is illegal to ask the voter to present identification, and thus an attacker can pretend to be some other registered voter.)

In our paper, we stated that: "As we noted in Section 3.1, some smartcards allow a user to get a listing of all the files on a card. If the system uses such a card and also uses the manufacturer's default password ..., then an attacker, even without any knowledge of the source code and without the ability to intercept the connection between a legitimate card and a voting terminal, but with access to a legitimate voter card, will still be able to learn enough about the smartcards to be able to create counterfeit voter cards." Diebold responded that all their voter cards do not use the manufacturer password. This makes the construction of homebrew cards harder for an adversary without knowledge of the source code and who doesn't want to or can't use a wire-tap device. That is good. But, as we pointed out above and in our paper, it is not unreasonable to assume that some other adversary might have access to the source code or a wire-tap device.

Diebold uses an insecure protocol that makes them vulnerable to counterfeit smartcards. Modern smartcards can perform cryptographic operations, allowing for more sophisticated protocols. If Diebold used such protocols, their system would be robust against our attacks.

What happens if an adversary (or adversaries) vote multiple times?

First, if an adversary votes multiple times, the tally of votes presented by the voting terminal will be incorrect. As we note in our paper: *If* there are no additional mechanisms to detect the presence of over-votes, then an adversary might successfully modify the outcome of the election. However, we are pleased to learn that (from Diebold's response): "before results are made official, the signatures are reconciled with the number of ballots cast on the voting machines. If the totals do not reconcile, an investigation is launched."

On page 10 of our paper we did note that "If we assume the number of collected votes becomes greater than the number of people who showed up to vote, and if the polling locations keep accurate counts of the number of people who show up to vote, then the back-end system, if designed properly, should be able to detect the existence of counterfeit votes." But, continuing in that same paragraph from page 10 of our report, "... there will be no way for the tabulating system to count the true number of voters or distinguish the real votes from the counterfeit votes. This would cast serious doubt on the validity of the election results." Diebold claims that if the existence of counterfeit votes were to be detected, an investigation would be launched. But what does that mean? It would seem impossible to call all the legitimate voters back to re-vote, especially if counterfeit votes were detected in a large number of precincts, and it is not clear that this is even legal. As we say in our paper, this could cast doubt on the validity of the election results. All it takes is for one person to figure out an attack for it to become widespread. On the Internet, most attacks are from so-called "Script Kiddies" who run malicious programs designed by others. This is the common method for attacks to spread, and so we must concern ourselves with what an intelligent, dedicated, and well-funded adversary could accomplish, as opposed to asking how sophisticated someone must be to launch this attack. Furthermore, it goes without saying that many people and organizations have a great amount at stake in an election. Voting systems must be robust against even the most sophisticated and well-funded adversary.

Software Engineering

Our original paper makes strong claims about Diebold's software engineering processes. We claim their coding standards are unsuitable for the security requirements that a voting terminal must face. Below we outline how we came to these conclusions.

In their response to "allegation 86," Diebold claims that their development process "followed common professional software engineering practice." This may very well be the case. However, building software that's intended to be secure, from day one, is different from traditional software engineering. Good designs start from an honest evaluation of the threats the system will face, and then a high-level design is gradually refined down into the specifics of the implementation. At each step of the process, the design needs to be carefully reviewed, and best practices should be employed to guarantee that high-level goals aren't lost in the translation to low-level code.

Diebold claims in their response to "allegation 78" that "the correctness of the software has been proven though [sic] an extensive testing process, both within the company and by independent testing authorities, and ultimately though [sic] logic and accuracy tests by the election officials themselves." Unlike traditional software engineering, where testing can be used to show that a feature functions correctly under normal circumstances, security engineering is concerned with *abnormal circumstances.* Thus, testing can only be used to show that a system is not vulnerable to a given set of attacks, not that a system is secure. Diebold also claims that in their "comprehensive top-to-bottom" code reviews they concentrate on "those parts of the code that tabulate vote results." Again, they are following software

design methodology and not security design methodology. Even if the code that is designed to tabulate the votes works correctly, that fact provides no information as to whether the vote tabulations can then be modified from some unassociated part of the code.

The correct way to design a secure system is to first identify the threats that such a system must defend against, then create detailed design documents that shows how each threat is mitigated. Only then can the design be implemented. This is the very same process mandated by the Department of Defense for certifying highly secure computer systems used to handle classified message traffic in the so-called Orange Book.

Maybe Diebold has some great high-level design documents. We never saw them, but we also never saw any reference to them in the source code. If the code were written in a truly rigorous fashion, you'd expect to see commentary in the code quoting chapter and verse from the design documents. It's just not there.

(For more information on how security engineering is fundamentally different from software engineering we refer the interested reader to Building Secure Software or Security Engineering.)

Furthermore, when building software that's meant to be robust against attacks, one of the most painful lessons of the past decade of computer science has been the damage that can be caused when a program is vulnerable to memory-corruption and type-confusion attacks (including the well known "buffer overflow"). These vulnerabilities are a special case of a general problem with the C and C++ programming languages (among others). These languages are not *memory safe* or *type safe*. While formally defining these terms is beyond the scope of this document, a programming language is *safe* if and only if no primitive operation in any program ever misinterprets data. For example, an integer is never misinterpreted as a pointer to a string. (This terminology is standard in the computer security and programming language communities; see this list for some examples). Such enforcement does not prevent all software bugs, but it does guarantee that a program's operation is predictable, and many important classes of bugs, including buffer overflows, can be *guaranteed* to never occur. Modern programming languages, including Java, C#, Ada, Modula-3, and many others have this important safety property. When Diebold's claims that "programming in any language can be safe or unsafe" (their responses to allegations 11, 71, and 72), they are really saying that they are unaware of one of the most fundamental improvements in software engineering since the invention of high-level programming. Even though Diebold criticizes our report for not "offering any evidence of such an exploit or failure" (their response to allegation 73), they cannot prove the *lack* of any such exploits or failures. Had they implemented their software with a modern programming language, such proof could be easily demonstrated.

Questions you can ask of vendors

Several people have asked us what questions they should be asking voting system vendors with regards to security. Here are some useful ones:

- Has your system been reviewed by a large number of outside security experts?
  - If so, who?
  - What are their credentials?
  - Do their areas of expertise cover a wide area of specialties within the discipline of cryptography and computer security?

  - Can we see an executive summary of their reports?

- Do you allow the public to review the security and reliability of your voting system's source code?
  - Is the security of your system dependent on your source code being secret?
  - If so, how do you address the fact that the source code could leak to the public (or to well-funded adversaries)?
  - And how do you address the fact that an attacker might be an insider who knows the source code?

- Would you be willing to have a panel of outside security experts review the source code for your system?
  - Would you allow them to publish an executive summary of their findings?
  - If not, why not?

- Who designed and developed the source code used in your systems?
  - What are their credentials with respect to cryptography and computer security?
  - Where were they trained?
  - Have these developers worked on cryptography and computer security in other systems outside of voting software?

- How confident are you in the security and reliability of your product? Will you "certify" the security and reliability of your product?
  - Will you offer a full refund, plus "damages," if somebody purchases your equipment and later find that it is vulnerable to certain types of attacks? (Which types of attacks?)
  - Will you offer a full refund, plus "damages," if after an election it is determined that more votes were collected than people who voted (on a given terminal), but that it cannot be determined which were the legitimate votes?
  - Will you offer a full refund, plus "damages," if after an election it is determined that your machines reported an inaccurate total (either because of an attack or a system glitch)?
  - Will you offer a full refund, plus "damages," if after an election it is determined that voters' anonymity was compromised, allowing votes to be bought and sold?
  - Under what other situations would you offer a full refund, plus "damages?"

- In your system, what can voters do if they feel that their votes were not recorded properly?
  - Are there any mechanisms for voters to verify their votes are correct?
  - What happens in the case of a dispute?
  - Is a manual recount (i.e., not requiring any computer software) possible?

- Does your system conform to the requirements of the Holt bill? Details can be found at http://holt.house.gov/issues2.cfm?id=5996.

Last updated August 1, 2003

The Case of the Diebold FTP Site

Part of the Voting and Elections web pages
by Douglas W. Jones
THE UNIVERSITY OF IOWA Department of Computer Science

Contents

For a summary of this story, as of Aug. 6, 2003, see . The Diebold AccuVote TS Should be Decertified.

---

1. Background

On Feb. 4, 2003, employees of Diebold Election Systems admitted that they had been using an insecure FTP server to exchange and update some part of Diebold's software. Bev Harris had discovered the server by doing a Google search, and she wrote it up in the on-line journal Scoop. [See Scoop, Feb 5, 2003 and Scoop, Feb 10, 2003] This FTP server was taken offline on Jan 29, and it is alleged to have contained files with names like "rob-georgia.zip", large parts of GEMS (the Global Election Management System), and unknown other software.

Not surprisingly, this disclosure fueled considerable speculation about some vast conspiracy undermining democracy. On April 23, 2003, Britain J. Williams, chair of the NASED Voting Systems Board Technical Committee, wrote a rebuttal to the charges raised by Bev Harris. [See the PDF or HTML versions of this letter] This letter is as a defense of the procedures used by the State of Georgia and the FEC/NASED certification process on which Georgia certification rests. [see the FEC and NASED websites] It shows, among other things, that Georgia has stronger defenses, in some respects, than my own state of Iowa.

The Williams letter assures voters that whatever was found on Diebold's FTP site is irrelevant to the conduct of elections in Georgia because the only path from that site into a voting machine is through the FEC/NASED process and Georgia's certification tests. The letter also contains a bit of

denial, for example, a statement that "the contents, or even existence, of the 'rob georgia' folder has not been established."

On July 8, 2003, Bev Harris posted the results of a preliminary examinaton of the files lifted from the Diebold FTP server. [See Scoop, July 8, 2003, Inside a U.S Election Vote Counting Program or Bev Harris's blackboxvoting.com web site; available in revised form from Bev Harris's blackboxvoting.org web site] The accompanying editorial, by the operators of the Scoop web site, included the the Internet address of a server from which this material could be downloaded and advice on how to crack the passwords. [See Scoop, July 8, 2003, Bigger than Watergate] The editorial urges people to make copies of the Diebold files and discuss what they find, and Harris created an on-line forum for this discussion of what was found. [See http://www.blackboxvoting.org/cgi-bin/dcforum/dcboard.cgi]

On July 9, Bev Harris posted specific rebuttals to the defense offered by Britain Williams in his April 23 letter. [See Scoop, July 10, 2003] This posting includes an extended transcript of an interview with Rob Behler, the 'rob' to whom the 'rob georgia' folder had been addressed. A more complete transcript of this interview is available. [See What really happened in Georgia? reposted at [IP] Interview with Georgia Diebold Election Machine installer] This interview makes it clear that the 'rob georgia' folder had nothing to do with an attempt to rob the state of Georgia, but it also makes it clear that the Georgia certification tests were, in reality, somewhat weaker than Williams had claimed, and that patches were indeed downloaded for these tests directly from the Diebold FTP site without passing through the FEC/NASED certification procedures, on the strength of a phone call to the source code auditor to determine that he wouldn't have considered the code in question to be subject to audit.

2. What We Already Knew

Prior to the disclosures and debate described above, we knew that Diebold Corporation had purchased Global Election Systems in 2001, which had purchased I-Mark Systems back in 1997; I-Mark was the original developer of the Electronic Ballot Station. Global had previously acquired the AccuVote mark-sense system, so naturally, they coined the name AccuTouch for the I-Mark Electronic Ballot Station. This system first passed through the FEC/NASED certification process on 9-10-96, in a kiosk configuration that incorporated CRT monitor. This original hardware was replaced by a portable flat-panel version that was certified on 12-5-97. That was the first version of the hardware I saw, when it came before the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems on Nov 6. 1997. [The minutes of this meeting indicate that Bob Urosevich and Barry Herron represented Global Election Systems at that meeting.] The sales material from Governmental Business Systems provides a good summary of the overall use of the Global System. [See http://www.gbsvote.com/wi/accuvotets.htm]

ISO 9000

Diebold has emphasized, in some of their presentations about this system, that it was developed under an ISO 9000 compliant development process. While it is worth noting that ISO 9000 does not guarantee quality in the product, it does demand use of a well-documented quality assurance system. The important thing is that the system is well documented and that management structures are in place to assure that it is used. ISO 9000 does not guarantee effective quality assurance, only that failures should be tracable to problems that should be evident in the documentation.

Compatability and Modes of Use

The Electronic Ballot Station, in both its kiosk form and its portable flat-panel form, is built from IBM PC compatable parts. In the now widely used flat-panel form, it consists of a wedge-shaped enclosure holding a PC motherboard, flat-panel display and various anciliaries including a smartcard reader, disk, network interface, and a compact internal uninterruptable power supply. Aside from packaging, it is a full featured PC, and when security seals are removed from the various ports on the side, it can be used as one by adding appropriate devices.

The same hardware that runs as an Electronic Ballot Station can also run other software, specifically, the Electronic Poll Book software. There are two practical ways to use the AccuTouch (or AccuVote Touchscreen System) in a polling place: In one, the polling place handles voter sign-in conventionally and has a stock of several hundred pre-recorded smartcards, each of which can be used to enable one voter to cast one ballot on an Electronic Ballot Station. In the other, each polling place has an Electronic Poll Book at the registration table that is used to record, on demand, the authorization card for each voter. Global originally suggested using the same hardware to run the Elecronic Poll Book as they use for the Electronic Ballot Station, but I believe it is as easy to use a commodity laptop with a commodity external smart-card interface for this function.

There is a third alternative to the above two. Originally, I-Mark Systems had intended what they called the "vote anywhere model". In this model, the voter registration cards sent to each voter would be smartcards, allowing a voter to walk up to any voting machine in the county and cast a vote using only his or her voter registration card. In the extreme discussed in early I-Mark sales literature, unattended kiosk-format Electronic Ballot Stations were to be available in public places such as libraries and shopping malls. I have not heard of any jurisdiction issuing smartcards to voters.

Use of Third-Party Commercial Off-the-Shelf Components

From the start, it was clear that the AccuTouch Electronic Ballot Station used a version of Windows and various Microsoft Office components. At the examination in Iowa on Nov 6, 1997, when asked about this, one of the representatives of Global stated, firmly, that the version of Windows they used was purely unmodified commercial off-the-shelf software, and therefore not subject to a source code audit under the FEC/NASED certification rules. [This must have been either Bob Urosevich or Barry Herron, the two company representatives who were present at that meeting.] I discussed potential problems with this in my testimony before the House Science Committee on May 22, 2001. [See Problems with Voting System Standards]

The FEC/NASED Voting System Standards require that all software used in voting systems be passed through a source-code audit, but there is an exemption, in both the 1990 and 2002 editions of this standard, for unmodified third-party 'COTS' software, that is, commercial off-the-shelf software produced by a third party that has not been modified for use in the voting context. Use of Microsoft Windows and Microsoft Office clearly qualifies for this exemption.

The standards do require, however, that all third-party components be documented! For hardware components, this typically means vendor, model, model number and revision number, and the same requirement should be applied to software. That is, the vendor should not be allowed to state merely that a product is approved for use on Microsoft Office, but rather, the vendor must state the version on which it has been certified, and a change of version should require recertification. There is an excellent examples of a revision to Windows that actually destroyed voter privacy on an early version of the Fidlar and Chambers direct recording electronic voting machine. I

discussed this example in my testimony before the House Science Committee cited above.

Unfortunately, the configuration documentation required by the FEC/NASED certification process is not public record, and in fact, all of the detailed technical documentation given by the vendor to the independent testing authority and the report of that independent testing authority is covered by nondisclosure agreements between the testers and the vendor. Only the fact of certification is public. Many states require configuration disclosure, however, and in many cases, these disclosures are, to varying extents, public. The states, however, have been sloppy and inconsistant about this! In Iowa, for example, it took us several years before we understood how partial the descriptions we were being given were; we have only recently begun to crack down on sloppy configuration disclosures, and to make a point of asking for model and revision numbers!

There is some debate about the word "unmodified". The narrowest interpretation would consider a third-party commercial off-the-shelf component to have been modified only if the source code for that component was changed. At the other extreme, any change to the out-of-the-box configuration of the component would count as modification. I suspect that extreme is wrong, but I also believe that the changes to the out-of-the-box configurations should be documented and subject to audit. If they claim to be using Microsoft Office XP with Service Pack 3, but with Word, Outlook, PowerPoint, FrontPage and SharePoint deleted, then this should be clearly stated and the audit should verify this configuration change.

Self Modifying Code

The FEC/NASED Voting System Standards explicitly forbid self-modifying code. There are several reasons for this prohibition, but the most important is the following: It is difficult to debug, prove the correctness of or audit software that is dynamically created at run-time. It is far easier to audit code that exists, in total, at the time of the audit.

There are disagreements about the nature of self-modifying code! Some would define it narrowly in terms of machine instructions that are overwritten by other instructions at run-time, while others define it broadly to include any dynamic linkage or interpretive execution, since all of these can be used to change the function of code after the fact.

Microsoft Windows makes extensive use of dynamically linked libraries and Microsoft Applications generally include interpreters for Visual Basic. In addition, it is natural to use mechanisms that border on interpretive for such things as formatting, as with HTML, or report generation, as with the ancient RPG language. The same considerations could lead to use of such mechanisms for ballot layout and canvassing, and in the past, it has been common for systems that border on being interpretive to evolve into fully developed general purpose interpreters; this happened with RPG. Depending on the interpretation of the restrictions on self-modification in the FEC/NASED Voting System Standards, use of these mechanisms could be problematic, and even if they are considered acceptable under the standards, their abuse introduces the possibility of security loopholes!

Communication and Security

AccuTouch Electronic Ballot Stations can be run in isolation, but the 1990 FEC/NASED Voting System Standards required that the totals for the precinct be automatically consolidated at the precinct, and this requires some communication between the machines at the precinct when more than one direct recording electronic voting machines is used. Some voting system vendors have

opted to use local area networks for this, notably Fidlar and Chambers (which became Fidlar Doubleday), while others have opted to use hand-carried cartridges of various sorts; Diebold uses PCMCIA cards, ES&S uses special and somewhat chunky custom built bricks).

Once the data for the precinct is consolidated, it may be printed at the precinct, as is required in many jurisdictions, and it may be transmitted by any of several communications options to the central offices, where precinct reports may be tabulated and printed using GEMS. Among these options are the option of hand carrying the precinct results in a PCMCIA card and the option of transmitting the results by modem.

Programming the AccuTouch machine for a particular election is also done using PCMCIA cards written on the GEMS system at the central offices and then loaded into the voting machine, and the permanent record of the election that is stored for recount purposes is stored on a PCMCIA card (with a duplicate record stored on the internal hard drive of the voting machine in case of failure). The 2002 Examination Report for the state of Washington contains a good summary of the use of PCMCIA cards on this system. [See Sam Reed report of Sept 6, 2002]

The security of all of these network links, including those involving hand carried data, is critical! It is noteworthy that PCMCIA cards are about the size of playing cards and we know that sleight of hand trickery with playing cards is a highly developed art, so cryptographic security of the data on these cards is just as essential as it is for data transmitted over a public network.

In additional discussion at the first Iowa examination of the AccuTouch system on Nov 6, 1997, it came out that neither the technical staff nor salespeople at Global Election Systems understood cryptographic security. They were happy to assert that they used the Federally approved Data Encryption Standard, but nobody seemed to understand key management, in fact, the lead programmer to whom my question was forwarded, by cell-phone, found the phrase *key management* to be unfamiliar and he needed explanation. On continued questioning, it became apparent that there was only one key used, company wide, for all of their voting products. The implication was that this key was hard-coded into their source code!

The minutes of the meeting reflect this discussion but do not mention the cellphone conversation:

> Dr. Jones also expressed concern about data encryption standards used to guarantee the integrity of the data on the machine. DES requires the use of electronic keys to lock and unlock all critical data. Currently all machines use the same key. Dr. Jones stated that this is a security problem. However, the use of a single key for all machines is not a condition that would disqualify the system under Iowa law.

The Iowa Secretary of State's office routinely forwards the minutes of these meetings to the vendor in question, so they did have both written and verbal notice of this serious security flaw; in addition, I wrote several paragraphs on this topic to the Elections Division of the Secretary of State's office on December 23, 1997:

> [This] raises another issue that reflects a weakness in both the FEC standards and Iowa law. This weakness has been clearly present in all of the electronic reporting systems we have examined this year! The Wyle report takes it for granted that the use of DES encryption plus CRC error checking provides a sufficient guarantee of accuracy and integrity.

Pages 6-36 available online

This paper, copyright the IEEE, appears in *IEEE Symposium on Security and Privacy 2004*. IEEE Computer Society Press, May 2004. This paper previously appeared as Johns Hopkins University Information Security Institute Technical Report TR-2003-19, July 23, 2003.

Analysis of an Electronic Voting System

TADAYOSHI KOHNO* ADAM STUBBLEFIELD† AVIEL D. RUBIN‡
DAN S. WALLACH§

February 27, 2004

Abstract

With significant U.S. federal funds now available to replace outdated punch-card and mechanical voting systems, municipalities and states throughout the U.S. are adopting paperless electronic voting systems from a number of different vendors. We present a security analysis of the source code to one such machine used in a significant share of the market. Our analysis shows that this voting system is far below even the most minimal security standards applicable in other contexts. We identify several problems including unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor software development processes. We show that voters, without any insider privileges, can cast unlimited votes without being detected by any mechanisms within the voting terminal software. Furthermore, we show that even the most serious of our outsider attacks could have been discovered and executed without access to the source code. In the face of such attacks, the usual worries about insider threats are not the only concerns; outsiders can do the damage. That said, we demonstrate that the insider threat is also quite considerable, showing that not only can an insider, such as a poll worker, modify the votes, but that insiders can also violate voter privacy and match votes with the voters who cast them. We conclude that this voting system is unsuitable for use in a general election. Any paperless electronic voting system might suffer similar flaws, despite any "certification" it could have otherwise received. We suggest that the best solutions are voting systems having a "voter-verifiable audit trail," where a computerized voting system might print a paper ballot that can be read and verified by the voter.

*Dept. of Computer Science and Engineering, University of California at San Diego, 9500 Gilman Drive, La Jolla, California 92093, USA. E-mail: tkohno@cs.ucsd.edu. URL: http://www-cse.ucsd.edu/users/tkohno. Most of this work was performed while visiting the Johns Hopkins University Information Security Institute. Supported by a National Defense Science and Engineering Graduate Fellowship.

†Information Security Institute, Johns Hopkins University, 3400 North Charles Street, Baltimore, Maryland 21218, USA. E-mail: astubble@cs.jhu.edu. URL: http://spar.isi.jhu.edu/~astubble.

‡Information Security Institute, Johns Hopkins University, 3400 North Charles Street, Baltimore, Maryland 21218, USA. E-mail: rubin@cs.jhu.edu. URL: http://www.avirubin.com.

§Dept. of Computer Science, Rice University, 3121 Duncan Hall, 6100 Main Street, Houston, Texas 77005, USA. E-mail: dwallach@cs.rice.edu. URL: http://www.cs.rice.edu/~dwallach.

Contents

1 Introduction

Elections allow the populace to choose their representatives and express their preferences for how they will be governed. Naturally, the integrity of the election process is fundamental to the integrity of democracy itself. The election system must be sufficiently robust to withstand a variety of fraudulent behaviors and must be sufficiently transparent and comprehensible that voters and candidates can accept the results of an election. Unsurprisingly, history is littered with examples of elections being manipulated in order to influence their outcome.

The design of a "good" voting system, whether electronic or using traditional paper ballots or mechanical devices, must satisfy a number of sometimes competing criteria. The *anonymity* of a voter's ballot must be preserved, both to guarantee the voter's safety when voting against a malevolent candidate, and to guarantee that voters have no evidence that proves which candidates received their votes. The existence of such evidence would allow votes to be purchased by a candidate. The voting system must also be *tamper-resistant* to thwart a wide range of attacks, including ballot stuffing by voters and incorrect tallying by insiders. Another factor, as shown by the so-called "butterfly ballots" in the Florida 2000 presidential election, is the importance of *human factors*. A voting system must be comprehensible to and usable by the *entire* voting population, regardless of age, infirmity, or disability. Providing accessibility to such a diverse population is an important engineering problem and one where, if other security is done well, electronic voting could be a great improvement over current paper systems. Flaws in any of these aspects of a voting system, however, can lead to indecisive or incorrect election results.

ELECTRONIC VOTING SYSTEMS. There have been several studies on using computer technologies to improve elections [4, 5, 20, 21, 25]. These studies caution against the risks of moving too quickly to adopt electronic voting machines because of the software engineering challenges, insider threats, network vulnerabilities, and the challenges of auditing.

As a result of the Florida 2000 presidential election, the inadequacies of widely-used punch card voting systems have become well understood by the general population. Despite the opposition of computer scientists, this has led to increasingly widespread adoption of "direct recording electronic" (DRE) voting systems. DRE systems, generally speaking, completely eliminate paper ballots from the voting process. As with traditional elections, voters go to their home precinct and prove that they are allowed to vote there, perhaps by presenting an ID card, although some states allow voters to cast votes without any identification at all. After this, the voter is typically given a PIN, a smartcard, or some other token that allows them to approach a voting terminal, enter the token, and then vote for their candidates of choice. When the voter's selection is complete, DRE systems will typically present a summary of the voter's selections, giving them a final chance to make changes. Subsequent to this, the ballot is "cast" and the voter is free to leave.

The most fundamental problem with such a voting system is that the entire election hinges on the correctness, robustness, and security of the software within the voting terminal. Should that code have security-relevant flaws, they might be exploitable either by unscrupulous voters or by malicious insiders. Such insiders include election officials, the developers of the voting system, and the developers of the embedded operating system on which the voting system runs. If any party introduces flaws into the voting system software or takes advantage of pre-existing flaws, then the results of the election cannot be assured to accurately reflect the votes legally cast by the voters.

Although there has been cryptographic research on electronic voting [13], and there are new approaches such as [6], currently the most viable solution for securing electronic voting machines is to introduce a "voter-verifiable audit trail" [10, 20]. A DRE system with a printer attachment, or even a traditional optical scan system (e.g., one where a voter fills in a printed bubble next to their chosen candidates), will satisfy this requirement by having a piece of paper for voters to read and verify that their intent is correct reflected. This paper is stored in ballot boxes and is considered to be the primary record of a voter's intent. If, for

some reason, the printed paper has some kind of error, it is considered to be a "spoiled ballot" and can be mechanically destroyed, giving the voter the chance to vote again. As a result, the correctness of any voting software no longer matters; either a voting terminal prints correct ballots or it is taken out of service. If there is any discrepancy in the vote tally, the paper ballots will be available to be recounted, either mechanically or by hand. (A verifiable audit trail does not, by itself, address voter privacy concerns, ballot stuffing, or numerous other attacks on elections.)

"CERTIFIED" DRE SYSTEMS. Many government entities have adopted paperless DRE systems without appearing to have critically questioned the security claims made by the systems' vendors. Until recently, such systems have been dubiously "certified" for use without any public release of the analyses behind these certifications, much less any release of the source code that might allow independent third parties to perform their own analyses. Some vendors have claimed "security through obscurity" as a defense, despite the security community's universally held belief in the inadequacy of obscurity to provide meaningful protection [18].

Indeed, the CVS source code repository for Diebold's AccuVote-TS DRE voting system recently appeared on the Internet. This appearance, announced by Bev Harris and discussed in her book, *Black Box Voting* [14], gives us a unique opportunity to analyze a widely used, paperless DRE system and evaluate the manufacturer's security claims. Jones discusses the origins of this code in extensive detail [17]. Diebold's voting systems are in use in 37 states, and they are the second largest and the fastest growing vendor of electronic voting machines. We only inspected unencrypted source code, focusing on the AVTSCE, or AccuVote-TS version 4, tree in the CVS repository [9]. This tree has entries dating from October 2000 and culminates in an April 2002 snapshot of version 4.3.1 of the AccuVote-TS system. From the comments in the CVS logs, the AccuVote-TS version 4 tree is an import of an earlier AccuTouch-CE tree. We did not have source code to Diebold's GEMS back-end election management system.

SUMMARY OF RESULTS. We discovered significant and wide-reaching security vulnerabilities in the version of the AccuVote-TS voting terminal found in [9] (see Table 1). Most notably, voters can easily program their own smartcards to simulate the behavior of valid smartcards used in the election. With such homebrew cards, a voter can cast multiple ballots without leaving any trace. A voter can also perform actions that normally require administrative privileges, including viewing partial results and terminating the election early. Similar undesirable modifications could be made by malevolent poll workers (or janitorial staff) with access to the voting terminals before the start of an election. Furthermore, the protocols used when the voting terminals communicate with their home base, both to fetch election configuration information and to report final election results, do not use cryptographic techniques to authenticate either end of the connection nor do they check the integrity of the data in transit. Given that these voting terminals could potentially communicate over insecure phone lines or even wireless Internet connections, even unsophisticated attackers can perform untraceable "man-in-the-middle" attacks.

We considered both the specific ways that the code uses cryptographic techniques and the general software engineering quality of its construction. Neither provides us with any confidence of the system's correctness. Cryptography, when used at all, is used incorrectly. In many places where cryptography would seem obvious and necessary, none is used. More generally, we see no evidence of disciplined software engineering processes. Comments in the code and the revision change logs indicate the engineers were aware of some areas in the system that needed improvement, though these comments only address specific problems with the code and not with the design itself. We also saw no evidence of any change-control process that might restrict a developer's ability to insert arbitrary patches to the code. Absent such processes, a malevolent developer could easily make changes to the code that would create vulnerabilities to be later exploited on Election Day. We also note that the software is written entirely in C++. When programming in a language like C++, which is not type-safe, programmers must exercise tight discipline to prevent their programs from being vulnerable to buffer overflow attacks and other weaknesses. Indeed, buffer overflows

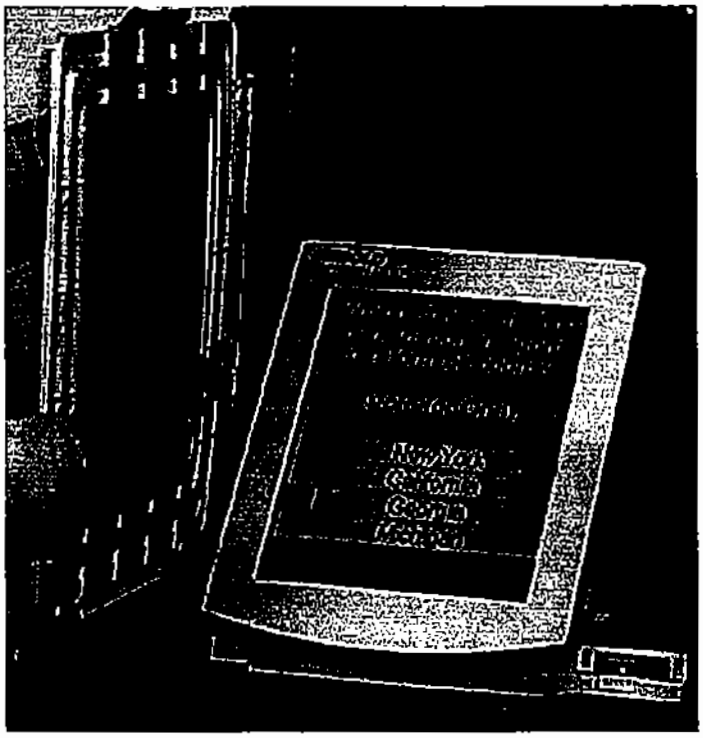


Figure 1: A Diebold AccuVote-TS voting machine (photo from `http://www.sos.state.ga.us/`). Note the smartcard reader in the lower-right hand corner.

caused real problems for AccuVote-TS systems in real elections.[1]

SUBSEQUENT WORK. Following the release of our results, the state of Maryland hired SAIC [27] and RABA [24] and the state of Ohio hired Compuware [7] to perform independent analyses of Diebold's AccuVote-TS systems. These analyses not only support our findings, but show that many of the issues we raise and attacks we identify still apply to recent versions of the AccuVote-TS system, and particularly to the machines recently purchased by Maryland. These analyses also identified security problems with the back-end GEMS server. Additionally, RABA's "red team" implemented some of our attacks in a mock election setting; e.g., they modified smartcards so that a voter could vote more than once (Section 3.2 and [24, page 16]) and they implemented our ballot reordering attack, thereby tricking voters to vote for the wrong candidates (Section 4.2 and [24, pages 18 and 21]). Jones discusses these three reports in more detail [17].

2 System overview

The Diebold AccuVote-TS 4.3.1 system we analyzed [9], which was written in C++, was designed to run on a Windows CE device, an example of which is shown in Figure 1. The code also compiles and runs (with slightly different configurations) on regular Microsoft Windows machines, thus enabling us to verify that the code represents a complete system. We shall refer to a device running the vote collection software as a *voting terminal*.

[1] `http://www.sccgov.org/scc/assets/docs/209815KeyboardAttachment-200440211.pdf` (page 60 of the report, page 61 of the PDF)

	Voter (with forged smartcard)	Poll Worker (with access to storage media)	Poll Worker (with access to network traffic)	Internet Provider (with access to network traffic)	OS Developer	Voting Device Developer	Section
Vote multiple times using forged smartcard	•	•	•				3.2
Access administrative functions or close polling station	•	•			•	•	3.3
Modify system configuration		•			•	•	4.1
Modify ballot definition (e.g., party affiliation)		•	•	•	•	•	4.2
Cause votes to be miscounted by tampering with configuration		•	•	•	•	•	4.2
Impersonate legitimate voting machine to tallying authority		•	•	•	•	•	4.3
Create, delete, and modify votes		•	•	•	•	•	4.3, 4.5
Link voters with their votes		•	•	•	•	•	4.5
Tamper with audit logs		•			•	•	4.6
Delay the start of an election		•	•	•	•	•	4.7
Insert backdoors into code					•	•	5.3

Table 1: This table summarizes some of the more important attacks on the system.

Below we describe the process for setting up and running an election using the Diebold system. In some cases, where election procedures and policies might vary or where we have insufficient information from studying the code, we will state our assumptions. We note that, even in cases where election policies and procedures might provide protection against design shortcomings, those policies and procedures depend on poll workers who may not fully understand or be able to carry out their responsibilities. As a result, any failure in the design of the voting system may very well be abused to compromise an election.

SETTING UP. Before an election takes place, one of the first things the election officials must do is specify the political offices and issues to be decided by the voters along with the candidates and their party affiliations. Variations on the ballot can be presented to voters based on their party affiliations. We call this data a *ballot definition*. In the Diebold system, a ballot definition is encoded as the file `election.edb`.

Prior to an election, the voting terminals must be configured and installed at each voting location. A governmental entity using Diebold voting terminals has a variety of choices in how to distribute the ballot definitions. They also may be distributed using removable media, such as floppy disks or storage cards, or over a local network, the Internet, or a dial-up connection. The networked approach, if allowed under the voting precinct's processes, provides additional flexibility to the election administrator in the event of last-minute changes to the ballot.

THE ELECTION. Once the voting terminal is initialized with the ballot definitions and the election begins, voters are allowed to cast their votes. To get started, the voter must have a *voter card*. The voter card is a memory card or smartcard; i.e., it is a credit-card sized plastic card with a computer chip on it that can store data and, in the case of the smartcard, perform computation. Under the most common scenario, we assume that the voting cards are given to voters at the voting site on election day.

The voter takes the voter card and inserts it into a smartcard reader attached to the voting terminal. The terminal checks that the smartcard in its reader is a voter card and, if it is, presents a ballot to the voter on the terminal screen. The actual ballot the voter sees may depend on the voter's political party, which is encoded on the voter card. If a ballot cannot be found for the voter's party, the voter is given a nonpartisan ballot. Such party-specific ballots are used, for example, in primaries.

At this point, the voter interacts with the voting terminal, touching the appropriate boxes on the screen for his or her desired candidates. Headphones and keypads are available for visually-impaired voters to privately interact with the terminal. Before the ballots are committed to storage in the terminal, the voter is given a final chance to review his or her selections. If the voter confirms this, the vote is recorded on the voting terminal and the voter card is "canceled." This latter step is intended to prevent the voter from voting again with the same card. After the voter finishes voting, the terminal is ready for another voter to use. The voter returns his or her canceled card to the poll workers, who reprogram it for the next user.

REPORTING THE RESULTS. A poll worker ends the election process by inserting an *administrator card* or an *ender card* (a special card that can only be used to end the election) into the voting terminal. Upon detecting the presence of such a card (and, in the case of the administrator card, checking a PIN entered by the card user), the poll worker is asked to confirm that the election is finished. If the poll worker agrees, then the voting terminal enters the post-election stage. Election results are written to a removable flash memory card and can also be transmitted electronically to the back-end server.

As we have only analyzed the code for the Diebold voting terminal, we do not know exactly how the back-end server tabulates the final results it gathers from the individual terminals. Obviously, it collects all the votes from the various voting terminals. We are unable to verify that there are checks to ensure, for example, that there are no more votes collected than people who are registered at or have entered any given polling location.

DETAILED OVERVIEW OF THE CODE. The 4.3.1 snapshot of the AccuVote-TS tree [9] has 136 `.h` files totaling 16414 lines and 120 `.cpp` files totaling 33195 lines, for a total of 256 files and 49609 lines of C++

code. While a full description of every module in the Diebold AccuVote-TS 4.3.1 system is beyond the scope of this paper, we describe the bootstrapping process as well as the main state transitions that occur within a Diebold system during an election, making explicit references to the relevant portions of the code.

The voting terminal is implemented in the directory `BallotStation/`, but uses libraries in the supporting directories `Ballot/`, `DES/`, `DiagMode/`, `Shared/`, `TSElection/`, `Utilities/`, and `VoterCard/`.

The method `CBallotStationApp::DoRun()` is the main loop for the voting terminal software. The `DoRun()` method begins by invoking `CBallotStationApp::LoadRegistry()`, which loads information about the voting terminal from the registry (the registry keys are stored under `HKEY_LOCAL_MACHINE\Software\Global Election Systems\AccuVote-TS4`). If the program fails to load the registry information, it believes that it is uninitialized and therefore creates a new instance of the `CTSRegistryDlg` class that asks the administrator to set up the machine for the first time. The administrator chooses, among other things, the COM port to use with the smartcard reader, the directory locations to store files, and the polling location identifier. The `CBallotStationApp::DoRun()` method then checks for the presence of a smartcard reader and, if none is found, gives the administrator the option to interact with the `CTSRegistryDlg` again.

The `DoRun()` method then enters a `while` loop that iterates until the software is shut down. The first thing `DoRun()` does in this loop is check for the presence of some removable media on which to store election results and ballot configurations (a floppy under Windows or a removable storage card on a Windows CE device). It then tries to open the election configuration file `election.edb`. If it fails to open the configuration file, the program enters the `CTSElectionDoc::ES_NOELECTION` state and invokes `CBallotStationApp::Download()`, which creates an instance of `CTransferElecDlg` to download the configuration file. To do the download, the terminal connects to a back-end server using either the Internet or a dial-up connection. Subsequently, the program enters the `CTSElectionDoc::ES_PREELECT` state, invoking the `CBallotStationApp::PreElect()` method, which in turn creates an instance of `CPreElectDlg`. The administrator can then decide to start the election, in which case `CPreElectDlg::OnSetForElection()` sets the state of the terminal to `CTSElectionDoc::ES_ELECTION`.

Returning to the while loop in `CBallotStationApp::DoRun()`, now that the machine is in the state `CTSElectionDoc::ES_ELECTION`, the `DoRun()` method invokes `CBallotStationApp::Election()`, which creates an instance of `CVoteDlg`. When a card is inserted into the reader, the application checks to see if the card is a voter card, administrator card, or ender card. If it is an ender card, or if it is an administrator card and if the user enters the correct PIN, the `CVoteDlg` ends and the user is asked whether he or she wishes to terminate the election and, if so, the state of the terminal is set to `CTSElectionDoc::ES_POSTELECT`. If the user entered a voter card, then `DoVote()` is invoked (here `DoVote()` is an actual function; it does not belong to any class). The `DoVote()` function finds the appropriate ballot for the user's voter group or, if none exists, opens the nonpartisan ballot (recall that the system is designed to support different ballots for different voters, as might occur in a primary party election). It then creates an instance of `CBallotDlg` to display the ballot and collect the votes.

We recall that if, during the election process, someone inserted an administrator or ender card into the terminal and chooses to end the election, the system would enter the `CTSElectionDoc::ES_POSTELECT` state. At this point the voting terminal would offer the ability to upload the election results to some back-end server for final tabulation. The actual transfer of results is handled by the `CTransferResultsDlg::OnTransfer()` method.

3 Smartcards

While it is true that one can design secure systems around the use of smartcards, merely the use of smartcards in a system does *not* imply that the system is secure. The system must use the smartcards in an intelligent and security-conscious way. Unfortunately, the Diebold system's use of smartcards provides very little (if any) additional security and, in fact, opens the system to several attacks.

3.1 Exploiting the lack of cryptography: Creating homebrew smartcards

Upon reviewing the Diebold code, we observed that the smartcards do not perform any cryptographic operations. This, in and of itself, is an immediate red flag. One of the biggest advantages of smartcards over classic magnetic-stripe cards is the smartcards' ability to perform cryptographic operations internally, and with physically protected keys. Because of a lack of cryptography, *there is no secure authentication of the smartcard to the voting terminal.* This means that nothing prevents an attacker from using his or her own homebrew smartcard in a voting terminal. One might naturally wonder how easy it would be for an attacker to make such a homebrew smartcard. First, we note that user-programmable smartcards and smartcard readers are available commercially over the Internet in small quantities and at reasonable prices. Second, an attacker who knows the protocol spoken between voting terminals and legitimate smartcards could easily implement a homebrew card that speaks the same protocol. We shall shortly consider how an attacker might go about learning the protocol if he or she does not know it *a priori*.

Once the adversary knows the protocol between the terminal and the smartcards, the only impediment to the mass production of homebrew smartcards is that each voting terminal will make sure that the smartcard has encoded in it the correct `m_ElectionKey`, `m_VCenter`, and `m_DLVersion` (see `DoVote()` in `BallotStation/Vote.cpp`). The `m_ElectionKey` and `m_DLVersion` are likely the same for all locations and, furthermore, for backward-compatibility purposes it is possible to use a card with `m_ElectionKey` and `m_DLVersion` undefined. The `m_VCenter` value could be learned on a per-location-basis by interacting with legitimate smartcards, from an insider, or from inferences based on the `m_VCenter` values observed at other polling locations. In short, all the necessary information to create homebrew counterfeit smartcards is readily available.

In the next subsections we consider attacks that an adversary could mount after creating homebrew cards. We find the issues we uncovered to be particularly distressing as modern smartcard designs allow cryptographic operations to be performed directly on the smartcard, making it possible to create systems that are not as easily vulnerable to such security breaches.

REVERSE ENGINEERING THE SMARTCARD PROTOCOL. It turns out that adversaries, including regular voters, who do not know *a priori* the protocol between the smartcard and the terminal can "easily" learn the protocol, thereby allowing them to produce homebrew voter cards. An adversary, such as a poll worker, with the ability to interact with a legitimate administrator or ender card could also learn enough information to produce homebrew administrator and ender cards (Section 3.3).

Let us consider several ways that an adversary could learn the protocol between voter cards and voting terminals. After voting, instead of returning the canceled card to the poll-worker, the adversary could return a fake card that records how it is reprogrammed, and then dumps that information to a collaborating attacker waiting in line to vote. Alternatively, the attacker could attach a "wiretap" device between the voting terminal and a legitimate smartcard and observe the communicated messages. The parts for building such a device are readily available and, depending on the setup at each voting location, might be unnoticed by poll workers. An attacker might not even need to use a wiretap device: as a literal "person-in-the-middle" attack, the adversary could begin by inserting a smartcard into the terminal that records the terminal's first message. The adversary would then leave the voting location, send that message to a real voter card that he or she stole, and learn the real voter card's response. The adversary's conspirator could then show up at the

voting location and use the information gained in the first phase to learn the next round of messages in the protocol, and so on. We comment again that these techniques work because the authentication process is completely deterministic and lacks any sort of cryptography.

3.2 Casting multiple votes

In the Diebold system, a voter begins the voting process by inserting a smartcard into the voting terminal. Upon checking that the card is "active," the voting terminal collects the user's vote and then deactivates the user's card; the deactivation actually occurs by rewriting the card's type, which is stored as an 8-bit value on the card, from `VOTER_CARD (0x01)` to `CANCELED_CARD (0x08)`. Since an adversary can make perfectly valid smartcards, the adversary could bring a stack of active cards to the voting booth. Doing so gives the adversary the ability to vote multiple times. More simply, instead of bringing multiple cards to the voting booth, the adversary could program a smartcard to ignore the voting terminal's deactivation command. Such an adversary could use one card to vote multiple times. Note here that the adversary could be a regular voter, and not necessarily an election insider.

Will the adversary's multiple-votes be detected by the voting system? To answer this question, we must first consider what information is encoded on the voter cards on a per-voter basis. The only per-voter information is a "voter serial number" (`m_VoterSN` in the `CVoterInfo` class). `m_VoterSN` is only recorded by the voting terminal if the voter decides *not* to place a vote (as noted in the comments in `TSElection/Results.cpp`, this field is recorded for uncounted votes for backward compatibility reasons). It is important to note that if a voter decides to cancel his or her vote, the voter will have the opportunity to vote again using that same card (and, after the vote has been cast, `m_VoterSN` will no longer be recorded).

If we assume the number of collected votes becomes greater than the number of people who showed up to vote, and if the polling locations keep accurate counts of the number of people who show up to vote, then the back-end system, if designed properly, should be able to detect the existence of counterfeit votes. However, because `m_VoterSN` is only stored for those who did not vote, there will be no way for the tabulating system to distinguish the real votes from the counterfeit votes. This would cast serious doubt on the validity of the election results. The solution proposed by one election official, to have everyone vote again, does not seem like a viable solution.

3.3 Accessing administrator and poll worker functionality

As noted in Section 2, in addition to the voter cards that normal voters use when they vote, there are also administrator cards and ender cards, which have special purposes in this system. The administrator cards give the possessor the ability to access administrative functionality (the administrative dialog `BallotStation/AdminDlg.cpp`), and both types of cards allow the possessor to end the election (hence the term "ender card").

Just as an adversary can manufacture his or her own voter cards, an adversary can manufacture his or her own administrator and ender cards (administrator cards have an easily-circumventable PIN, which we will discuss shortly). This attack is easiest if the attacker has knowledge of the Diebold code or can interact with a legitimate administrator or ender card, since otherwise the attacker would not know what distinguishes an administrator or ender card from a voter card. (The distinction is that, for a voter card `m_CardType` is set to `0x01`, for an ender card the value is `0x02`, and for an administrator card the value is `0x04`.)

As one might expect, an adversary in possession of such illicit cards has further attack options against the Diebold system. Using a homebrew administrator card, a poll worker, who might not otherwise have access to the administrator functions of the Diebold system but who does have access to the voting machines before and after the elections, could gain access to the administrator controls. If a malicious voter entered an

administrator or ender card into the voting device instead of the normal voter card, then the voter would be able to terminate the election and, if the card is an administrator card, gain access to additional administrative controls.

The use of administrator or ender cards prior to the completion of the actual election represents an interesting denial-of-service attack. Once "ended," the voting terminal will no longer accept new voters (see `CVoteDlg::OnCardIn()`) until the terminal is somehow reset. Such an attack, if mounted simultaneously by multiple people, could temporarily shut down a polling place. If a polling place is in a precinct considered to favor one candidate over another, attacking that specific polling place could benefit the less-favored candidate. Even if the poll workers were later able to resurrect the systems, the attack might succeed in deterring a large number of potential voters from voting (e.g., if the attack was performed over the lunch hour). If such an attack was mounted, one might think the attackers would be identified and caught. We note that many governmental entities, e.g., California, do not require identification to be presented by voters. By the time the poll workers realize that one of their voting terminals has been disabled, the perpetrator may have long-since left the scene. Furthermore, the poll workers may not be computer savvy and might simply think that all the machines crashed simultaneously.

CIRCUMVENTING THE ADMINISTRATOR PIN. In order to use (or create) an administrator card, the attacker must know the PIN associated (or to be associated) with the card. Because the system's use of smartcards was poorly designed, an adversary could easily learn the necessary information, thereby circumventing any security the PIN might have offered.

We first note that the PIN is sent from the smartcard to the terminal in cleartext. As a result, anyone who knows the protocol and wishes to make their own administrator card could use any PIN of their choice. Even if the attacker does not know the protocol but has access to an existing administrator card and wants to make a copy, the adversary could guess the PIN in just a few trials if the adversary realizes that the PIN is included as part of a short cleartext message sent from the card. More specifically, rather than try all 10000 possibilities for the PIN, the adversary could try all 4-byte consecutive substrings of the cleartext message.

4 Election configurations and election data

In election systems, protecting the integrity and privacy of critical data (e.g., votes, configurations, ballot definitions) is undeniably important. We investigated how the Diebold system manipulates such data, and found considerable problems. There are two main vectors for accessing and attacking the voting system's data: via physical access to the device storing the data, or via man-in-the-middle attacks as the data is transported over some network. The latter assumes that the systems are connected to a network, which is possible though may be precluded by election procedures in some jurisdictions. Attacks via physical access to memory can be quite powerful, and can be mounted easily by insiders. The network attacks, which can also be quite powerful, can also be mounted by insiders as well as sophisticated outsiders.

DATA STORAGE OVERVIEW. Each voting terminal has two distinct types of internal data storage. A main (or system) storage area contains the terminal's operating system, program executables, static data files such as fonts, and system configuration information, as well as backup copies of dynamic data files such as the voting records and audit logs. Each terminal also contains a removable flash memory storage device that is used to store the primary copies of these dynamic data files. When the terminal is running a standard copy of Windows (e.g., Windows 2000) the removable storage area is the first floppy drive; when the terminal is running Windows CE, the removable storage area is a removable storage card. Storing the dynamic data on two distinct devices is advantageous for both reliability and non-malleability: if either of the two storage mediums fails, data can still be recovered from the copy, although reconciling differences between these media may be difficult.

Unfortunately, in Windows CE, the existence of the removable storage device is not enforced properly.

Unlike other versions of Windows, removable storage cards are mounted as subdirectories under CE. When the voting software wants to know if a storage card is inserted, it simply checks to see if the `Storage Card` subdirectory exists in the filesystem's root directory. While this is the default name for a mounted storage device, it is also a perfectly legitimate directory name for a directory in the main storage area. Thus, if such a directory exists, the terminal can be fooled into using the same storage device for all of the data.[2] This would reduce the amount of redundancy in the voting system and would increase the chances that a hardware failure could cause recorded votes to be lost.

NETWORK OVERVIEW. The Diebold voting machines cannot work in isolation. They must be able to both receive a ballot definition file as input and report voting results as output. As described in Section 2, there are essentially two ways to load a voting terminal with an initial election configuration: via some removable media, such as a flash memory card, or over a network connection. In the latter case, the voting terminal could either be plugged directly into the Internet, could be connected to an isolated local network, or could use a dialup connection (the dial-up connection could be to a local ISP, or directly to the election authority's modem banks). Diebold apparently gives their customers a variety of configuration options; electronic networks are not necessary for the operation of the system. After the election is over, election results can be sent to a back-end post-processing server over the network (again, possibly through a dial-up connection). When results are reported this way, it is not clear whether these network-reported results become the official results, or just the preliminary results (the official results being computed after the memory cards are removed from all the voting terminals and collected and tabulated at a central location).

We also observe that, even in jurisdictions where voting terminals are *never* connected to a network or phone line, the physical transportation of the flash memory cards from the voting terminal to the central tabulating system is really just a "sneaker net." Such physical card transportation must be robust against real-world analogies of network man-in-the-middle attacks. Any flaws in the policies and procedures used to protect the chain of custody could lead to opportunities for these cards to be read or written by an adversary. Consequently, even if no electronic computer network is used, we still view network attacks as critical in the design of a voting system.

4.1 Tampering with the system configuration

The majority of the system configuration information for each terminal is stored in the Windows registry under `HKEY_LOCAL_MACHINE\Software\Global Election Systems\AccuVote-TS4`. This includes both identification information such as the terminal's serial number and more traditional configuration information such as the COM port to which the smartcard reader is attached. All of the configuration information is stored in the clear, without any form of integrity protection. Thus, all an adversary must do is modify the system registry to trick a given voting terminal into effectively impersonating any other voting terminal. It is unclear how the tabulating authority would deal with results from two different voting terminals with the same voting ID; at the very least, human intervention to resolve the conflict would probably be required.

The Federal Election Commission draft standard [11] requires each terminal to keep track of the total number of votes that have ever been cast on it — the "Protective Counter." This counter is used to provide yet another method for ensuring that the number of votes cast on each terminal is correct. However, as the following code from `Utilities/machine.cpp` shows, the counter is simply stored as an integer in the file `system.bin` in the terminal's system directory (error handling code has been removed for clarity):

```
long GetProtectedCounter()
```

[2] This situation can be easily corrected by checking for the `FILE_ATTRIBUTE_TEMPORARY` attribute on the directory as described in `http://msdn.microsoft.com/library/en-us/wcefiles/htm/_wcesdk_Accessing_Files_on_Other_Storage_Media.asp`.

```
{
  DWORD protectedCounter = 0;
  CString filename = ::GetSysDir();
  filename += _T("system.bin");
  CFile file;
  file.Open(filename, CFile::modeRead | CFile::modeCreate | CFile::modeNoTruncate);
  file.Read(&protectedCounter, sizeof(protectedCounter));
  file.Close();
  return protectedCounter;
}
```

We believe that the Diebold system violates the FEC requirements by storing the protected counter in a simple, mutable file. By modifying this counter, an adversary could cast doubt on an election by creating a discrepancy between the number of votes cast on a given terminal and the number of votes that are tallied in the election. While the current method of implementing the counter is totally insecure, even a cryptographic checksum would not be enough to protect the counter; an adversary with the ability to modify and view the counter would still be able to roll it back to a previous state. In fact, the only solution that would work would be to implement the protective counter in a tamper-resistant hardware token, but doing so would require physical modifications to existing hardware.

4.2 Tampering with ballot definitions

The "ballot definition" for each election (`election.edb`) contains everything from the background color of the screen and information about the candidates and issues on the ballot to the PPP username and password to use when reporting the results, if reporting the results over a dial-up connection. This data is neither encrypted nor checksummed (cryptographically or otherwise).

If uninterrupted physical access is *ever* available to the voting terminal after the ballot definition has been loaded, perhaps the night before an election, using a janitor's master keys to the building, then it would be possible for an adversary to tamper with the voting terminals' ballot definition file or to even tamper with the voting software itself. Protections such as physical locks or tamper-evident seals may somewhat allay these concerns, but we would prefer designs that can be robust even against physical tampering.

On a potentially much larger scale, if the voting terminals download the ballot definition over a network connection, then an adversary could tamper with the ballot definition file en-route from the back-end server to the voting terminal; of course, additional poll-worker procedures could be put in place to check the contents of the file after downloading, but we prefer a technological solution. With respect to modifying the file as it is sent over a network, we point out that the adversary need not be an election insider; the adversary could, for example, be someone working at the local ISP. If the adversary knows the structure of the ballot definition, then the adversary can intercept and modify the ballot definition while it is being transmitted. Even if the adversary does not know the precise structure of the ballot definition, many of the fields inside are easy to identify and change, including the candidates' names, which appear as plain ASCII text.

Because no cryptographic techniques are in place to guard the integrity of the ballot definition file, an attacker could add, remove, or change issues on the ballot, and thereby confuse the result of the election. In the system, different voters can be presented with different ballots depending on their party affiliations (see `CBallotRelSet::Open()`, which adds different issues to the ballot depending on the voter's `m_VGroup1` and `m_VGroup2` `CVoterInfo` fields). If an attacker changes the party affiliations of the candidates, then he may succeed in forcing the voters to view and vote on erroneous ballots.[3] More subtle

[3] As an example of what might happen if the party affiliations were listed incorrectly, we note that, according to a news story at `http://www.gcn.com/vol19_no33/news/3307-1.html`, in the 2000 New Mexico presidential election, over 65,000 votes were incorrectly counted because a worker accidentally had the party affiliations wrong. (We are not claiming this worker had malicious intent, nor are we implying that this error had an effect on the results of the election.)

attacks are also possible. By simply changing the order of the candidates as they appear in the ballot definition, the results file will change accordingly. However, the candidate information itself is not stored in the results file, which merely tracks that candidate 1 got so many votes and candidate 2 got so many other votes. If an attacker reordered the candidates on the ballot definition, voters would unwittingly cast their ballots for the wrong candidate. Ballot reordering attacks would be particularly effective in polling locations known to have more voters of one party than another. (In Section 4.3 and Section 4.5 we consider other ways of tampering with the election results.)

4.3 Impersonating legitimate voting terminals

Consider voting terminals that are configured to upload voting totals to some back-end tabulating authority after an election. An adversary able to pose as a legitimate voting terminal to the tabulating authority could obviously cause (at least temporary) damage by reporting false vote counts to the tabulating system. If the voting terminals use a normal Internet connection, then an adversary with the ability to sniff the connection of a legitimate terminal could learn enough information (e.g., the IP address of the back-end server) to be able to impersonate a legitimate terminal. If the terminals use a dialup connection, then the adversary would either need to be able to sniff a legitimate dialup connection to learn the appropriate information (e.g., the dial-up PPP number, login, and password), or must garner that information in another way. The PPP phone number, username, password, and IP address of the back-end server are stored in the registry `HKEY_LOCAL_MACHINE\Software\Global Election Systems\AccuVote-TS4\TransferParams`, thus making it easily accessible to an insider working at the polling station. By studying the configuration of the ballot definition files, we learned that the definition files also store the terminal's voting center ID, PPP dial-in number, username, password and the IP address of the back-end server (these are parsed into a `CElectionHeaderItem` in `TSElection\TSElectionObj.cpp`). The ballot definition files thus provide another vector for an adversary to learn almost all of the information necessary to impersonate a real voting terminal over a dialup connection (the adversary would also have to create a voting terminal ID, although the ID may or may not be checked for legitimacy by the back-end server).

4.4 Key management and other cryptographic issues with the vote and audit records

Unlike the other data stored on the voting terminal, both the vote records and the audit logs are encrypted and checksummed before being written to the storage device. Unfortunately, neither the encrypting nor the checksumming is done with established, secure techniques. This section summarizes the issues with Diebold's use of cryptography in protecting the vote records and audit logs, and then return to consequences of Diebold's poor choices in subsequent subsections. (Recall that we have already discussed the lack of cryptography in other potions of the system.)

KEY MANAGEMENT. All of the data on a storage device is encrypted using a single, hardcoded DES [22] key:

```
#define DESKEY ((des_key*)"F2654hD4")
```

Note that this value is not a hex representation of a key, nor does it appear to be randomly generated. Instead, the bytes in the string "`F2654hD4`" are fed directly into the DES key scheduler. It is well-known that hardcoding keys into a program's source code is a bad idea: if the same compiled program image is used on every voting terminal, an attacker with access to the source code, or even to a single program image, could learn the key and thus read and modify voting and auditing records. The case with the Diebold system is even worse: from the CVS logs, we see this particular key has been used without change since December 1998, when the CVS tree for AccuVote-TS version 3 began, and we assume that the key was in use much before

that. Although Jones reports that the vendor may have been aware of the key management problems in their code since at least 1997 [16, 17], our findings show that the design flaw was never addressed. The SAIC analysis of Diebold's system [27] agrees that Diebold needs to redesign their cryptography architecture. The most appropriate solution will likely involve the use of hardware cryptographic coprocessors.

(In a similar fashion, Diebold's voter, administrator, and ender cards use a hardcoded 8-byte password ED 0A ED 0A ED 0A ED 0A (hexadecimal) to authenticate the voting terminals to the smartcards, transmitted in cleartext. The smartcards are discussed in Section 3.)

"ENCRYPTION." Even if proper key management were to be implemented, however, many problems would still remain. First, DES keys can be recovered by brute force in a very short time period [12]. DES should be replaced with either triple-DES [26] or, preferably, AES [8]. Second, DES is being used in CBC mode which requires a random initialization vector to ensure its security. The implementation here always uses zero for its IV. This is illustrated by the call to `DesCBCEncrypt` in `TSElection/RecordFile.cpp`; since the second to last argument is NULL, `DesCBCEncrypt` will use the all-zero IV.

```
DesCBCEncrypt((des_c_block*)tmp, (des_c_block*)record.m_Data, totalSize,
              DESKEY, NULL, DES_ENCRYPT);
```

To correctly implement CBC mode, a source of "strong" random numbers must be used to generate a fresh IV for each encryption [2]. Suitably strong random numbers can be derived from many different sources, ranging from custom hardware to accumulated observations of user behavior.

"MESSAGE AUTHENTICATION." Before being encrypted, a 16-bit cyclic redundancy check (CRC) of the plaintext data is computed. This CRC is then stored along with the ciphertext in the file and verified whenever the data is decrypted and read. This process in handled by the `ReadRecord` and `WriteRecord` functions in `TSElection/RecordFile.cpp`. Since the CRC is an unkeyed, public function, it does not provide any meaningful integrity protection for the data. In fact, by storing it in an unencrypted form, the purpose of encrypting the data in the first place (leaking no information about the contents of the plaintext) is undermined. Standard industry practice would be to first encrypt the data to be stored and then to compute a keyed cryptographic checksum (such as HMAC-SHA1 [1]) of the ciphertext [3, 19]. This cryptographic checksum could then be used to detect any tampering with the plaintext. Note also that each entry has a timestamp, which can be used to detect reordering, although sequence numbers should also be added to detect record deletion.

4.5 Tampering with election results and linking voters with their votes

A likely attack target are the voting records themselves. When stored on the device, the voting records are "encrypted" as described in Section 4.4. If the votes are transmitted to a back-end authority over a network connection, as appears to be the case in at least some areas, no cryptography is used: the votes are sent in cleartext. In particular, `CTransferResultsDlg::OnTransfer()` writes ballot results to an instance of `CDL2Archive`, which then writes the votes in cleartext to a socket without any cryptographic checksum. If the network connection is via a cable modem or a dedicated connection, then the adversary could be an employee at the local ISP. If the voting terminals use a dialup connection directly to the tabulating authority's network, then the risk of such an attack is less, although still not inconsequential. A sophisticated adversary, e.g., an employee of the local phone company, could tap the phone line and intercept the communication.

TAMPERING WITH ELECTION RESULTS. In Section 4.2 we showed that an adversary could alter election results by modifying ballot definition files, and in Section 4.3 we showed that an adversary could inject fake votes to a back-end tabulating authority by impersonating a legitimate voting terminal. Here we suggest another way to modify the election result: modify the voting records file stored on the device. Because of the poor cryptography described in Section 4.4, an attacker with access to this file would be able to

generate or change as many votes as he or she pleased. Furthermore, the adversary's modified votes would be indistinguishable from the true votes cast on the terminal. The attack described here is more advantageous to an adversary than the attacks in Section 4.2 and Section 4.3 because it leaves no evidence that an attack was ever mounted (whereas the attacks in Section 4.2 and Section 4.3 could be discovered but not necessarily corrected as part of a post-election auditing phase).

If the votes are sent to the back-end authority over a network, then there is another vector for an adversary to modify the election results. Specifically, an adversary with the ability to tamper with the channel could introduce new votes or modify existing votes. Such an attacker could, for example, decrease one candidate's vote count by some number while increasing another's candidate's count by the same number. Of course, to introduce controlled changes such as these to the votes, the attacker would benefit from some knowledge of the structure of the protocol used between the terminals and the back-end server. This form of tampering might later be detected by comparing the memory storage cards to data transmitted across the networks, although the memory storage cards themselves might also be subject to tampering. (We briefly comment that these network attacks could be largely circumvented with the use of standard cryptographic tools, such as SSL/TLS.)

LINKING VOTERS WITH THEIR VOTES. From analyzing the code, we learned that each vote is written *sequentially* to the file recording the votes. This fact provides an easy mechanism for an attacker, such as a poll worker with access to the voting records, to link voters with their votes. A poll worker could surreptitiously track the order in which voters use the voting terminals. Later, in collaboration with other attackers who might intercept the "encrypted" voting records, the exact voting record of each voter could be reconstructed.

If the results are transmitted over a network, as is the case in at least some jurisdictions, then physical access to the voting results is not even necessary. Recall that, when transmitted over the network, the votes are sent in unencrypted, cleartext form.

"RANDOMIZED" SERIAL NUMBERS. While the voter's identity is not stored with the votes, each vote is given a serial number in order to "randomize" the votes after they are uploaded to the back-end tabulating authority. As we noted above, randomizing the order of votes *after* they are uploaded to the the tabulating authority does not prevent the possibility of linking voters to their votes. Nevertheless, it appears that the designers wanted to use a cryptographically secure pseudorandom number generator to generate serial numbers for some post-processing purposes. Unfortunately, the pseudorandom number generator they chose to use (a linear congruential generator) is not cryptographically secure. Moreover, the generator is seeded with static information about the voting terminal and the election.

```
// LCG - Linear Conguential Generator - used to generate ballot serial numbers
// A psuedo-random-sequence generator
// (per Applied Cryptography, by Bruce Schneier, Wiley, 1996)
#define LCG_MULTIPLIER 1366
#define LCG_INCREMENTOR 150889
#define LCG_PERIOD 714025

static inline int lcgGenerator(int lastSN)
{
  return ::mod(((lastSN * LCG_MULTIPLIER) + LCG_INCREMENTOR), LCG_PERIOD);
}
```

It is interesting to note that the code's authors apparently decided to use an linear congruential generator because it appeared in *Applied Cryptography* [26] even though in the same work it is advised that such generators should not be used for cryptographic purposes.

4.6 Audit logs

Each entry in a plaintext audit log is simply a timestamped, informational text string. There appears to be no clear pattern for what is logged and what is not. The whole audit log is encrypted using the insecure method described in Section 4.4. An adversary with access to the audit log file could easily change its contents.

At the time that the logging occurs, the log can also be printed to an attached printer. If the printer is unplugged, off, or malfunctioning, no record will be stored elsewhere to indicate that the failure occurred. The following code from `TSElection/Audit.cpp` demonstrates that the designers failed to consider these issues:

```
if (m_Print && print) {
  CPrinter printer;
  // If failed to open printer then just return.
  CString name = ::GetPrinterPort();
  if (name.Find(_T("\\")) != -1)
    name = GetParentDir(name) + _T("audit.log");
  if (!printer.Open(name, ::GetPrintReverse(), FALSE))
    ::TSMessageBox(_T("Failed to open printer for logging"));
  else {
    [ do the printing ]
  }
}
```

If the cable attaching the printer to the terminal is exposed, an attacker could create discrepancies between the printed log and the log stored on the terminal by unplugging the printer (or, by simply cutting the cable).

4.7 Attacking the start of an election

Although good election processes would dictate installing the ballot definition files well before the start of the election, we can imagine scenarios in which the election officials must reinstall ballot files shortly before the start of an election, and do not have time to distribute the definition files manually.[4]

One option for the election officials would be to download the files over the Internet. In addition to the problems we have outlined, we caution against relying on such an approach, as an adversary could mount a traditional Internet denial-of-service attack against the election management's server and thereby prevent the voting terminals from acquiring their ballot definition files in time for the election. Even a general idea of the range of Internet addresses used by the election administration would be sufficient for an attacker to target a large-scale distributed denial of service (DDoS) attack.

Of course, we acknowledge that there are other ways to postpone the start of an election at a voting location that do not depend on Internet DDoS attacks (e.g., flat tires for all poll workers for a given precinct, or other acts of real-world vandalism). Unlike such traditional attacks, however, (1) the network-based attack is relatively easy for anyone with knowledge of the election system's network topology to accomplish; (2) this attack can be performed on a very large scale, as the central distribution point(s) for ballot definitions becomes an effective single point of failure; and (3) the attacker can be physically located anywhere in the Internet-connected world, complicating efforts to apprehend the attacker. Such attacks could prevent or delay the start of an election at all voting locations in a state. We note that this attack is not restricted to the system we analyzed; it is applicable to any system that downloads its ballot definition files using the Internet or otherwise relies upon the Internet.

[4] In recent elections, we have seen cases where politicians passed away or withdrew from the race very close to the election day.

5 Software engineering

When creating a secure system, getting the design right is only part of the battle. The design must then be securely implemented. We now examine the coding practices and implementation style used to create the voting system. This type of analysis can offer insights into future versions of the code. For example, if a current implementation has followed good implementation practices but is simply incomplete, one would be more inclined to believe that future, more complete versions of the code would be of a similar high quality. Of course, the opposite is also true, perhaps even more so: it is very difficult to produce a secure system by building on an insecure foundation.

Of course, reading the source code to a product gives only an incomplete view into the actions and intentions of the developers who created that code. Regardless, we can see the overall software design, we can read the comments in the code, and, thanks to the CVS repository, we can even look at earlier versions of the code and read the developers' commentary as they committed their changes to the archive.

5.1 Code legacy

Inside `cvs.tar` we found multiple CVS archives. Two of the archives, `AccuTouch` and `AVTSCE`, implement full voting terminals. The `AccuTouch` code, corresponding to AccuVote-TS version 3, dates from December 1998 to August 2001 and is copyrighted by "Global Election Systems, Inc.," while the `AVTSCE` code, corresponding to the AccuVote-TS version 4 system, dates from October 2000 to April 2002 and is copyrighted by "Diebold Election Systems, Inc." (Diebold acquired Global Election Systems in September 2001.[5]) Although the `AccuTouch` tree is not an immediate ancestor of the `AVTSCE` tree (from the CVS logs, the `AVTSCE` tree is actually an import of another `AccuTouch-CE` tree that we do not have), the `AccuTouch` and `AVTSCE` trees are related, sharing a similar overall design and a few identical files. From the comments, some of the code, such as the functions to compute CRCs and DES, date back to 1996 and a company later acquired by Global Election Systems called "I-Mark Systems." We have already remarked (Section 4.4) that the same DES key has been hardcoded into the system since at least the beginning of the `AccuTouch` tree.

5.2 Coding style

While the system is implemented in an unsafe language[6] (C++), the code reflects an awareness of avoiding such common hazards as buffer overflows. Most string operations already use their safe equivalents, and there are comments, e.g., `should really use _snprintf`, reminding the developers to change others. While we are not prepared to claim that there are no exploitable buffer overflows in the current code, there are at the very least no glaringly obvious ones. Of course, a better solution would have been to write the entire system in a safe language, such as Java or Cyclone [15]. In such a language we would be able to prove that large classes of attacks, including buffer overflows and type-confusion attacks, are impossible assuming a correct implementation of the compiler and runtime system.

Overall, the code is rather unevenly commented. While most files have a description of their overall function, the meanings of individual functions, their arguments, and the algorithms within are more often than not undocumented. An example of a complex and completely undocumented function is the `CBallotRelSet::Open` function from `TSElection/TSElectionSet.cpp` as shown in Figure 2. This block of code contains two nested loops, four complex conditionals, and five debugging assertions, but no comments that explain its purpose. Ascertaining the meaning of even a small part of this code is a huge undertaking. For example, what does it mean for `vgroup->KeyId() == -1`? That the ID is simply

[5] `http://dallas.bizjournals.com/dallas/stories/2001/09/10/daily2.html`

[6] Here we mean language safety in the technical sense: no primitive operation in any program ever misinterprets data.

```
void CBallotRelSet::Open(const CDistrict* district, const CBaseunit* baseunit,
                                    const CVGroup* vgroup1, const CVGroup* vgroup2)
{
   ASSERT(m_pDB != NULL);
   ASSERT(m_pDB->IsOpen());
   ASSERT(GetSize() == 0);
   ASSERT(district != NULL);
   ASSERT(baseunit != NULL);

   if (district->KeyId() == -1) {
      Open(baseunit, vgroup1);
   } else {
      const CDistrictItem* pDistrictItem = m_pDB->Find(*district);
      if (pDistrictItem != NULL) {
         const CBaseunitKeyTable& baseunitTable = pDistrictItem->m_BaseunitKeyTable;
         int count = baseunitTable.GetSize();
         for (int i = 0; i < count; i++) {
            const CBaseunit& curBaseunit = baseunitTable.GetAt(i);
            if (baseunit->KeyId() == -1 || *baseunit == curBaseunit) {
               const CBallotRelationshipItem* pBalRelItem = NULL;
               while ((pBalRelItem = m_pDB->FindNextBalRel(curBaseunit, pBalRelItem))){
                  if ((!vgroup1 || vgroup1->KeyId() == -1 ||
                     (*vgroup1 == pBalRelItem->m_VGroup1 && !vgroup2) ||
                     (vgroup2 && *vgroup2 == pBalRelItem->m_VGroup2 &&
                        *vgroup1 == pBalRelItem->m_VGroup1))
                      Add(pBalRelItem);
               }
            }
         }
         m_CurIndex = 0;
         m_Open = TRUE;
      }
   }
}
```

Figure 2: The function `CBallotRelSet::Open` function from `TSElection/TSElectionSet.cpp`. This complex function is completely undocumented.

undefined? Or perhaps that the group should be ignored? Such poorly documented code impairs the ability of both internal developers and external security evaluator to assess whether the code is functioning properly or might lead to a security issue.

5.3 Coding process

An important point to consider is how code is added to the system. From the project's CVS logs, we can see that most recent code updates are in response to specific bugs that needed to be fixed. There are, however, no references to tracking numbers from a bug database or any other indication that such fixes have been vetted through any change-control process. Indeed, each of the programmers[7] seem to have completely autonomous authority to commit to any module in the project. The only evidence that we have found that the code undergoes any sort of review comes from a single log comment: "Modify code to avoid multiple exit points to meet Wyle requirements." This refers to Wyle Labs, one of the independent testing authorities charged with certifying that voting machines have met FEC guidelines.

Virtually any serious software engineering endeavor will have extensive design documents that specify how the system functions, with detailed descriptions of all aspects of the system, ranging from the user interfaces through the algorithms and software architecture used at a low level. We found no such documents in the CVS archive, and we also found no references to any such documents in the source code, despite references to algorithms textbooks and other external sources.

There are also pieces of the voting system that come from third parties. Most obviously, a flaw in the operating system, Windows CE, could expose the system to attack since the OS controls memory manage-

[7]Through web searches, we have matched each programmer's CVS user names with their likely identities and so can conclude that they are not group accounts.

ment and all of the device's I/O needs. In addition, an audio library called *fmod* is used.[8] While the source to *fmod* is available with commercial licenses, unless this code is fully audited it might contain a backdoor or an exploitable buffer overflow. Since both the operating system and *fmod* can access the memory of the voting program, both must be considered part of the trusted computing base (TCB) as a security vulnerability in either could compromise the security of the voting program itself. The voting terminal's hardware boot instructions should likewise be considered part of the TCB.

Due to the lack of comments, the legacy nature of the code, and the use of third-party code and operating systems, we believe that any sort of comprehensive, top-to-bottom code review would be nearly impossible. Not only does this increase the chances that bugs exist in the code, but it also implies that any of the coders could insert a malicious backdoor into the system without necessarily being caught. The current design deficiencies provide enough other attack vectors, however, that such an explicit backdoor is not required to successfully attack the system. Regardless, even if the design problems are eventually rectified, the problems with the coding process may well remain intact.

Since the initial version of this paper was made available on the Internet, Diebold has apparently "developed, documented, and implemented a change control process" [27]. The details of this revised process have not been made available to the public, so we are unable to comment on their effectiveness.

5.4 Code completeness and correctness

While the code we studied implements a full system, the implementors have included extensive comments on the changes that would be necessary before the system should be considered complete. It is unclear whether the programmers actually intended to go back and remedy all of these issues as many of the comments existed, unchanged, for months, while other modifications took place around them. Of course, while the AVTSCE code we examined appears to have been the current codebase in April 2002, we know nothing about subsequent changes to the code. (Modification dates and locations are easily visible from the CVS logs.) These comments come in a number of varieties. For illustrative purposes, we have chosen to show a few such comments from the subsystem that plays audio prompts to visually-impaired voters.

- Notes on code reorganization:
```
/* Okay, I don't like this one bit.  Its really tough to tell where m_AudioPlayer
should live.  [...]  A reorganization might be in order here.  */
```
- Notes on parts of code that need cleaning up:
```
/* This is a bit of a hack for now.  [...]  Calling from the timer message
appears to work.  Solution is to always do a 1ms wait between audio clips.  */
```
- Notes on bugs that need fixing:
```
/* need to work on exception *caused by audio*.  I think they will currently
result in double-fault.  */
```

There are, however, no comments that would suggest that the design will radically change from a security perspective. None of the security issues that have been discussed in this paper are pointed out or marked for correction. In fact, the only evidence at all that a redesign might at one point have been considered comes from outside the code: the Crypto++ library[9] is included in another CVS archive in `cvs.tar`. However, the library was added in September 2000, before the start of the AVTSCE AccuVote-TS version 4 tree, and appears to have never been used. (The subsequent SAIC [27] and RABA [24] analyses report that many of the problems we identify are still applicable to recent versions of the AccuVote-TS system, implying

[8] `http://www.fmod.org/`

[9] `http://www.eskimo.com/~weidai/cryptlib.html`

that, at least up to the version that SAIC and RABA analyzed, there has not been any radical change to the AccuVote-TS system.)

6 Conclusions

Using publicly available source code, we performed an analysis of the April 2002 snapshot of Diebold's AccuVote-TS 4.3.1 electronic voting system. We found significant security flaws: voters can trivially cast multiple ballots with no built-in traceability, administrative functions can be performed by regular voters, and the threats posed by insiders such as poll workers, software developers, and janitors is even greater. Based on our analysis of the development environment, including change logs and comments, we believe that an appropriate level of programming discipline for a project such as this was not maintained. In fact, there appears to have been little quality control in the process.

For quite some time, voting equipment vendors have maintained that their systems are secure, and that the closed-source nature makes them even more secure. Our glimpse into the code of such a system reveals that there is little difference in the way code is developed for voting machines relative to other commercial endeavors. In fact, we believe that an open process would result in more careful development, as more scientists, software engineers, political activists, and others who value their democracy would be paying attention to the quality of the software that is used for their elections. (Of course, open source would not solve all of the problems with electronic elections. It is still important to verify somehow that the binary program images running in the machine correspond to the source code and that the compilers used on the source code are non-malicious. However, open source is a good start.) Such open design processes have proven successful in projects ranging from very focused efforts, such as specifying the Advanced Encryption Standard (AES) [23], through very large and complex systems such as maintaining the Linux operating system. Australia is currently using an open source voting system[10].

Alternatively, security models such as the voter-verified audit trail allow for electronic voting systems that produce a paper trail that can be seen and verified by a voter. In such a system, the correctness burden on the voting terminal's code is significantly less as voters can see and verify a physical object that describes their vote. Even if, for whatever reason, the machines cannot name the winner of an election, then the paper ballots can be recounted, either mechanically or manually, to gain progressively more accurate election results. Voter-verifiable audit trails are required in some U.S. states, and major DRE vendors have made public statements that they would support such features if their customers required it. The EVM project[11] is an ambitious attempt to create an open-source voting system with a voter-verifiable audit trail — a laudable goal.

The model where individual vendors write proprietary code to run our elections appears to be unreliable, and if we do not change the process of designing our voting systems, we will have no confidence that our election results will reflect the will of the electorate. We owe it to ourselves and to our future to have robust, well-designed election systems to preserve the bedrock of our democracy.

Acknowledgments

We thank Cindy Cohn, David Dill, Badri Natarajan, Jason Schultz, Tracy Volz, David Wagner, and Richard Wiebe for their suggestions and advice. We also thank the state of Maryland for hiring SAIC and RABA and the state of Ohio for hiring Compuware to independently validate our findings.

[10] `http://www.elections.act.gov.au/EVACS.html`

[11] `http://evm2003.sourceforge.net`

References

[1] M. Bellare, R. Canetti, and H. Krawczyk. Keying hash functions for message authentication. In N. Koblitz, editor, *Advances in Cryptology – CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 1–15. Springer-Verlag, Berlin Germany, Aug. 1996.

[2] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A concrete security treatment of symmetric encryption. In *Proceedings of the 38th Annual Symposium on Foundations of Computer Science*, pages 394–403. IEEE Computer Society Press, 1997.

[3] M. Bellare and C. Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In T. Okamoto, editor, *Advances in Cryptology – ASIACRYPT 2000*, volume 1976 of *Lecture Notes in Computer Science*, pages 531–545. Springer-Verlag, Berlin Germany, Dec. 2000.

[4] California Internet Voting Task Force. *A Report on the Feasibility of Internet Voting*, Jan. 2000. `http://www.ss.ca.gov/executive/ivote/`.

[5] *Voting: What Is; What Could Be*, July 2001. `http://www.vote.caltech.edu/Reports/`.

[6] D. Chaum. Secret-ballot receipts: True voter-verifiable elections. *IEEE Security and Privacy*, 2(1):38–47, 2004.

[7] Compuware Corporation. *Direct Recording Electronic (DRE) Technical Security Assessment Report*, Nov. 2003. `http://www.sos.state.oh.us/sos/hava/files/compuware.pdf`.

[8] J. Daemen and V. Rijmen. *The Design of Rijndael: AES–The Advanced Encryption Standard*. Springer-Verlag, Berlin Germany, 2002.

[9] Diebold Election Systems. `AVTSCE` source tree, 2003. `http://users.actrix.co.nz/dolly/Vol2/cvs.tar`.[12]

[10] D. L. Dill, R. Mercuri, P. G. Neumann, and D. S. Wallach. *Frequently Asked Questions about DRE Voting Systems*, Feb. 2003. `http://www.verifiedvoting.org/drefaq.asp`.

[11] Federal Election Commission. *Voting System Standards*, 2001. `http://fecweb1.fec.gov/pages/vss/vss.html`.

[12] J. Gilmore, editor. *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design*. O'Reilly, July 1998.

[13] D. Gritzalis, editor. *Secure Electronic Voting*. Springer-Verlag, Berlin Germany, 2003.

[14] B. Harris. *Black Box Voting: Vote Tampering in the 21st Century*. Elon House/Plan Nine, July 2003.

[15] T. Jim, G. Morrisett, D. Grossman, M. Hicks, J. Cheney, and Y. Wang. Cyclone: A safe dialect of C. In *USENIX Annual Technical Conference*, June 2002.

[16] D. W. Jones. *Problems with Voting Systems and the Applicable Standards*, May 2001. Testimony before the U.S. House of Representatives' Committee on Science, `http://www.cs.uiowa.edu/~jones/voting/congress.html`.

[12] The `cvs.tar` file has been removed from this website.

how saintly those two corporations might be. However, the reality is that these two corporations are ES&S and Diebold, and they offer us other reasons for our misgivings–ranging from the hiring of felons to write their software, to their numerous broken promises–and finally to the lawsuits filed against them for the insufficiency of their products.

It is important to note that when ownership of our public systems remain under the domain of the government, the government must achieve higher standards for public scrutiny, e.g. the government cannot hide its software behind "Trade Secret" laws.

5 **False Dilemmas:** Our election officials are now seeking to comply with the equipment purchase deadlines mandated by the Help America Vote Act ("HAVA"), but they're offered a false dilemma on what to do with these HAVA millions:
Use it now *(before good options are available)* **or lose it!**

Yet there is a third way, particularly, when **the spirit of the Help America Vote Act** ("HAVA") was to improve our voting systems and not merely exchange one broken system for another on the pretense of meeting HAVA and EAC deadlines. (Notably, the Election Assistance Commission itself has been tardy in providing guidelines and HAVA has been late in funding.) California can provide a leadership role in the responsible implementation of HAVA.

6 **Caveat Emptor: Hang on to those HAVA Millions!** Many citizens are unaware of the true cost of the new voting methods. The spending of our nearly $400 million HAVA budget primarily on equipment will be a mere **down-payment** on the true cost. For example, much of this extremely pricey equipment is guaranteed only for the short term and requires expensive private maintenance contracts, as well as poll worker training. In some instances the new paper trail compliant systems require the vendor's own personnel to read the coiled-up paper trails.

We recommend that the State of California NOT squander OUR hundreds of millions of taxpayer dollars–our HAVA budget–on any new equipment that does not meet responsible election integrity standards.

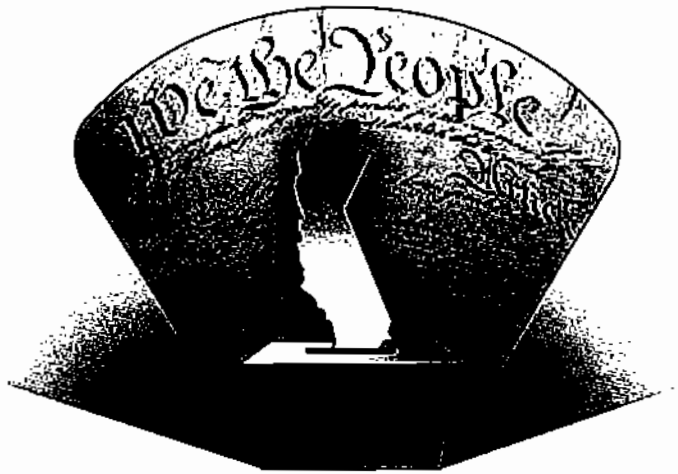
In the event there is no acceptable equipment to purchase now, common sense dictates that we save the majority of our money for the near future when better options become available. Let's not let our HAVA money burn a hole in our pockets.

In the meantime, inexpensive optical scan technology with shuffle-able paper ballots is readily available in every precinct, or easy to attain at comparatively low prices. Also, a wealth of information on what HAVA really mandates can be found in ***"Mythbreakers"*** by VotersUnite.org (free on their website).

We can do better than mortgage our children's future with payment plans that will likely continue long past the exhaustion of the HAVA funds, and so we shall.

Democracy for America-Marin http://www.dfamarin.org/

California's Voting Integrity



We Can Do It Right!

1 Security Leaks: Transparent and secure voting systems are a requisite for a bona fide democracy. Yet to date our citizens are offered only insecure "Trade Secret" guarded voting systems.

Our voting systems are more than the voting box–they are the entire journey from the moment a person registers through to final tabulation.

If our current options for voting systems were compared to our drinking water plumbing systems, the vulnerabilities, the leaks, would likely render the tap undrinkable. *Why?* Potential vulnerabilities are numerous and more are exposed daily, but here are a few notable examples:

- **A sham federal qualification program, which receives 1/3 of its funding from e-vendors:** The federal qualification rules are vague, the compliance is inconsistent, and the results are unreliable.
- **Voting system *vendor security* trumps *vote security*:** Even Kevin Shelley in the capacity of Secretary of State for the State of California could not get essential information on voting equipment from those entrusted with federal qualification on the grounds that the information was deemed "Trade Secret."
- **Security vulnerabilities susceptible to tampering:** Even in cases of "stand alone" paper voting systems with no connectivity, these systems can easily switch over to act as a "Trojan Horse" as soon as "features" are later added. For example, the previously secure InkaVote system in Los Angeles has now been rendered insecure by the addition of a wireless feature harboring untenable security risks.
- **Our democracy must rely upon *"faith-based"* voting systems:** The public has no proof of the security of our current voting systems, yet the legal concept of *"res ipsa loquitur"* ("the thing speaks for itself") places the burden of proof on the manufacturer when it is impossible for citizens to attain inside knowledge, e.g. "Trade Secret" guarded software, limited component access.

2 Unreliable Product: Our democratic body cannot survive without a clean voting system any more than our bodies can survive without a clean water system. Yet in both cases, even if we cannot fix all the system vulnerabilities to contamination, we can at least test the final product before relying on it.

The checking of the final product of a voting system–*BEFORE* relying on it–assures our citizenry that our election integrity standards are worthy of the lives lost in the name of democracy. Cindy Sheehan, co-founder of the Gold Star Families for Peace (mother of slain solidier Casey Sheehan) stated the need, as follows:

"Non-verifiable electronic voting has already made a farce of the election process in certain parts of the US. Anyone who doesn't advocate the use of easy to read paper ballots, ballots that can be handled with hands, seen with eyes, stored in boxes for recount and verification, and with some sealing mechanism to protect against tampering, either doesn't know how fraudulent vote tabulating has already become in certain parts of the country, or they favor the results already gained through fraud."

3 What's the Solution Now? Auditability Equals Legitimacy: Not one more election in California ***BEFORE*** our election integrity issues are satisfied–period! The following protocol will offer our citizens checks and balances that their vote is counted as cast:

Accessible, voter-verifiable, **paper** ballots on archival paper that are able to be shuffled to retain secrecy of the sequence of voting, along with a "**Gold Star Audit**" that has these five points as its requirements:

1 **When:** mandatory audits of ALL elections

2 **What *(Step one)*:** genuinely random sampling of, at a minimum, 5%* of all precincts

3 **What *(Step two)*:** Within the random sampling above, recount 100% of the paper ballots (or paper audit trails)

4 **How:** Hand-counted

5 **Who & Where:** Non-partisan oversight in a public forum

* This is minimum figure subject to change if credible scientific information suggests an increase is prudent.

4 Ownership. Absolute power corrupts absolutely, and this warning caused an unprecedented number of U.S. citizens to cry foul when FCC Chair Michael Powell attempted to give control over OUR public trust, our public airways, to the a handful of corporations that would then control 80% of the media.

Today our democracy is at issue: 80% of our U.S. vote counting is controlled by just TWO corporations. This is an untenable security threat to our democracy–no matter

Item #1

The Diebold TSx with AccuView is Prematurely on the Agenda

The Procedures for approval of a voting system require a complete Application to be submitted before examination may begin. This was not done. According to the Executive Summary Addendum written June 7 all the required reports have not been received.

The staff's June 6 report (p.6) claims that GEMS 1.18.22 has completed federal qualification testing to 2002 Voting System Standards. They even have claimed to have the reports on file. Yet Mr. Freeman's June 7 report (p.4) states that the final test reports for GEMS version 1.18.22 have not been received from either the hardware or software ITAs. Mr. Freeman even concludes his summary by making his recommendations conditional "pending receipt of the ITA reports". This is the same sequence of events that occurred in October and November 2003 when Diebold kept promising the reports and qualification numbers would shortly be issued. Even the elections staff themselves assured the VSP panel that everything was qualified and the number would be issued at any moment. Nearly two years later and the same tactics are still being utilized to get a system California approved.

As of June 15, NASED reports that GEMS 1.18.22 has not been qualified to 2002 Voting System Standards. In fact, every Diebold voting system with a NASED Qualification Number is only qualified to 1990 Voting System Standards.

Additionally, as part of the requirements, the Final Draft Procedures are required to be submitted 45 days prior to the VSP hearing. That was not done.

Does the Elections Division ignore the requirement for a complete application before starting the examination process for all vendors, or just some? After Diebold's behavior the last time they tried to push through the certification process without having met all the requirements, I would think the Elections Division would be more cautious with Diebold's assurances.

This agenda item should not be considered for certification because it is premature according to the requirements of the Secretary's Procedures. The examination should start after the application is complete, and the hearing should not occur until after the other requirements are met.

OBJECTIONS TO DEIBOLD GEMS 1.18.22/AV-TSX 4.6.1 VOTING SYSTEM with The AccuView Printer Module

AVVPAT Issues

1. Printed on Thermal Paper
   Limited Shelf life, will not meet 22 month ballot storage Requirements
   Over sensitive to heat- can be damaged by improper storage and transportation
   Hot conditions, inside trucks, can damage paper and compromise its integrity
   Readability Issue, Thermal printing is hard to read on the first day, gets worse each successive day
2. Size of AVVPAT- this is so small, that a magnifying glass is necessary,
   Voters deserve better that a gas station sized and quality type of Voter Verified Paper Audit Trail
   Excessively small size of AVVPAT is inherently non-conducive to access and use. It creates an immediate obstacle to its use and intended purpose. Instead of being user friendly, it becomes user avoidance and is a direct hindrance to the entire concept of AVVPAT.
3. Size of AVVPAT must be of normal size equal to the traditional size of a traditional ballot, which provides ease of use and a normalization standard and level of familiarity to All voters
4. Voters deserve more than a flimsy, unreadable gas station receipt to verify their Voting Choices
5. Use of a magnifying glass to verify the voters choices on the Diebold AVVPAT
   This is an insult to each and every voter and to the American Voting Process
6. Failure of the Magnifying Glass to display the bottom lines of the ballot image.
   This is unacceptable, to the voter and to Democracy
7. Size of the AVVPAT-since less than perfect 20-20 Eyesight is quite prevalent within the general population, this small size is difficult, if not impossible to read, making the entire concept of any AVVPAT sized smaller than a normal, traditional ballot totally unacceptable. This size is prejudicial and discriminates against a significant number of voting citizens with a common form of a physical disability.
8. AVVPAT must be printed on traditional ballot sized paper by an ink jet printer.
9. The take up reel and operational functions of the paper tape AVVPAT are not fully functional and are predisposed to failure and breakdown when used in the day long voting process.
10. If a Form of AVVPAT is unusable, inaccessible, and unreadable by a significant percentage of the voting population, it is a failure as being "Voter Verified" and "Auditable" There are 30 organizations who Agree
11. Violation and Imposition of Section 19214.5 of the California Election Code
    Due to Diebold's violation of Subsection (a)-by their fraudulent sale of claimed Federal qualification status and their sale and use by 17 California counties of said Fraudulently uncertified and switched software, we demand that ANY Diebold equipment NOT be certified for use in California, and further more that as per Subsection (3) be prohibited from doing business in California for 3 years.

Petition to the California Secretary of State

As Diebold has misled the State of California many times in the past and has provided uncertified software for use in elections, and as the use of Diebold equipment has disenfranchised voters by forcing late opening of polls in the March, 2004 election, and as Diebold's proposed paper trail is costly, unsuitable for recounts, and does not protect the confidentiality of the voters because it preserves the order in which ballots were cast,

Be it resolved that in order to protect the integrity of elections in California, restore citizen confidence in the electoral system, and provide transparency to the electoral system, the Secretary of State must not certify Diebold Election Systems for use in California. Further, as authorized by section 192104.5 (a) (3) of the California Elections Code, the Secretary of State must ban Diebold from doing any elections-related business in the state for three years.

In addition, counties with existing Diebold equipment should evaluate alternatives for compliance with the Help America Vote Act of 2002 and the California Elections Code rather than solely negotiating upgrades to existing Diebold systems.

Name	City	County	Zip Code	e-mail (print clearly)
Eileen Moodie	Roseville	Placer	95747	emoodie@lanset.com
WESLEY CLARK	ROSEVILLE	PLACER	95661	WESCLARK@SUREWEST.NET
Charles Brown	Roseville	Placer	95678	chasdbrown@hotmail.com
JOHN O'DONNELL	ORANGEVALE	SACRAMENTO	95662	jgodonnel@comcast.net
Mary Clark	ROSEVILLE	Placer	95661	marweo@surewest.net
Paul Wertenberger	Roseville	Placer	95661	paulmarkw@yahoo.com
Windy Wertenberger	Roseville	Placer	95661	windy96@excite.com
Glenda Wertenberger	Roseville	Placer	95661	paulindaw@yahoo.com
Nancy Tilcock	Rocklin	Placer	95677	NT
Diana Malcolm	Rocklin	Placer	95765	guenevere@sbcglobal.net

For more information, or to sign on-line, and for how to help, go to **http://election-reform.us/**
Bring printed petitions to the VSPP hearing or return petitions to:
Jerry Berkman
3136 Eton Avenue
Berkeley, California 94705

Office of the Secretary of State
Clean Voting System
16 June 05

Having voted since 1960 and knowing the exit polls are always reliable, I knew instantly when the exit polls in the 2004 general election did not match the black box tabulation that something was very wrong.

This became increasingly apparent as time went on and there was absolutely no logical explanation: The huge discrepancies were in the "black box tabulation".

There is not a breathing American who can call himself a true American without insisting on a clean and fair election.

That has not happened in the last two general elections.

We need to make this voting system CLEAN NOW because our representative democracy is already in trouble.

Jerry Ann Campbell
California registered voter

El Dorado County

THE CASE FOR FRAUD IN THE 2004 ELECTION

David Benavides, 18 May 2005

The single most important issue of our times is the question of vote fraud. This essay demonstrates beyond any reasonable doubt that something went terribly wrong in the November 2, 2004 Presidential election. Whether you accept or reject the fraud thesis, you are compelled to review the evidence if you take our democracy seriously. Given that the mainstream media refuses to discuss the fraud possibility, not only is the "right of the people to choose their representatives" under attack but the second pillar of democracy, "freedom of the press" appears to be under siege.

PART I

WE NO LONGER LIVE IN A DEMOCRACY

The United States of America lost its claim to being a democracy with the 2000 election of George W. Bush.

The official story put out by the mass media points to a close election in Florida where Bush beat Gore by a couple of hundred votes. The Florida Supreme Court ordered a recount, but the U.S. Supreme Court over-ruled Florida, handing Bush a victory. Two dissenting U.S. Supreme Court Justices, John Paul Stevens and Ruth Bader Ginsburg, stated that the highest court in the land had "no legal basis" for intervening in the election since election processes are managed by each state according to the United States Constitution. Even if we accept the "the close vote story", the election of GWB was illegal.

The real story is that Governor Jeb Bush and Florida Secretary of State Katherine Harris hired ChoicePoint, a private company, to remove the names of 100,000 Florida voters from the rolls, predominately in minority areas in Miami-Dade county, who would have voted sixty percent for Gore. In short, Gore would have beaten Bush easily by 20,000 votes.

This act of treason by Republicans in fixing the 2000 election was surpassed by the complicity of the Democratic Party: not one Senator joined the Black Congressional caucus in protesting Florida's electoral votes during the January 2001 certification process. This was the real shame of the USA: the Party of the people sold out and refused to fight for democracy!

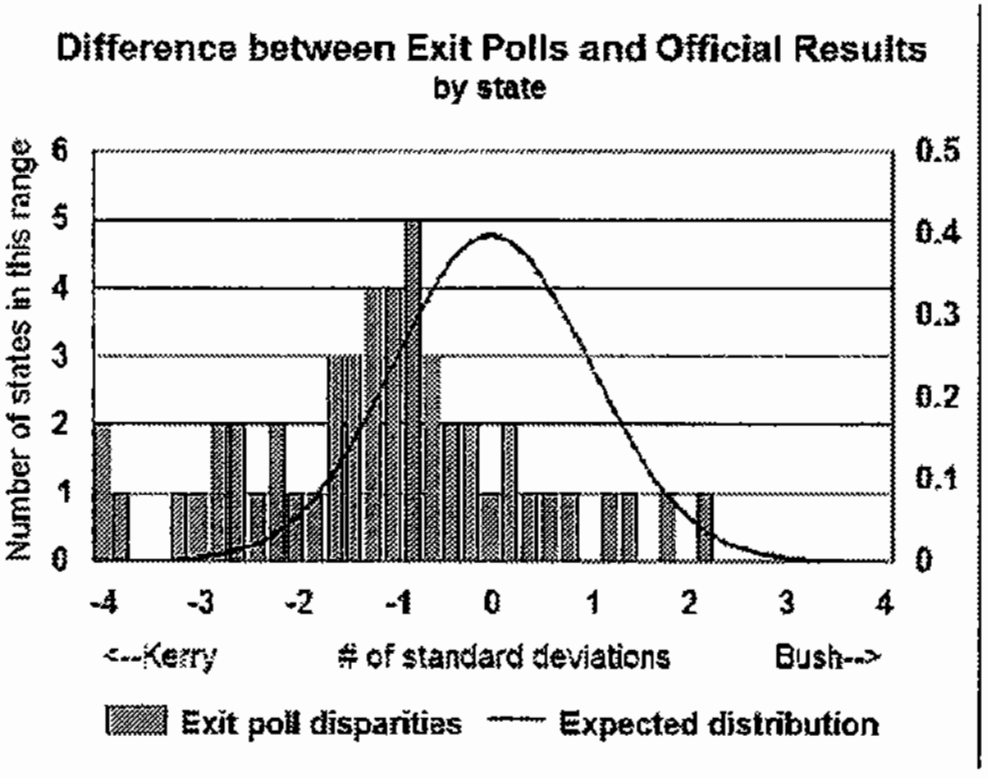
Democratic weakness emboldened the Republicans who set out to fix the 2004 election, projecting their domination for another four years both in the House and Senate. The trick was to use the Florida vote-counting fiasco as an excuse to move to electronic voting throughout the USA. Republicans achieved their goal when sixty five percent of the 160 million votes on November 2, 2004 were counted on electronic machines throughout the USA with half of these being "paperless" direct

electronic recording, voting machines (DREs) without any possibility of doing a recount. To underscore their intentions, Jeb Bush stated before the election: "There will be no recount in Florida".

The proof for the fixing of the 2004 election is ample and extensive. It can be found throughout the internet websites. One of the best is Gary Beckwith's http://election.solarbus.org/ . There you will find several major scientific studies by leading scholars which demonstrate beyond any reasonable doubt that Bush did NOT win the electoral vote (e.g. he did NOT win Ohio and Florida) or the popular vote. The Executive Summary of the definitive report, "Response to the Report Evaluation of Edison/Mitofsky Election System 2004", by the US Count Votes' National Election Data Archive Project is located at http://electionarchive.org/ucvAnalysis/US/Exit_Polls_summary.pdf . **It can be paraphrased as follows:**

1- **The weighted national exit poll, conducted by Edison/Mitofsky, predicted Kerry to win the popular vote by 3 % but the official vote count had Bush winning by 2.5 %. This discrepancy of 5.5 % is the largest in the poll's history, representing 5 million less votes for Kerry and 3 million excess votes for Bush: a total of 8 million stolen votes.**

2- **Seven of fifty states (DE;MN;NH;NY;VT;SC;PA) have t values less than – 2.7, meaning that each of their discrepancies had less than 1 % probability of occurring by chance. The probability that 7 of 50 states should be so skewed is less than 1 in 10 million:**



This means that random error must be ruled out as an explanation for the difference between election results and exit polls. Only two other possibilities remain: bias in the exit polling process or a systematic stealing of votes from Kerry and their transfer to Bush. For the bar graphs to be this far away from zero in the normal bell curve means that something was way off -either the exit polls or the official vote count. Edison/Mitofsky International agreed that something was definitely wrong and stated it was their own nationwide exit polls.

3- **Edison/Mitofsky concoct a story that Bush voters were "shy/reluctant to answer the pollsters" and therefore, there was a systematic bias in the polling process since, within the 70,000 nationwide respondents, Kerry voters were over-sampled. The US Count Votes study demonstrates that Edison/Mitosky's own polling data does not and cannot support this fabrication. In fact, the Edison/Mitosky data supports the opposite conclusion: (1) response to exit polls were slightly higher in Republican precincts compared to Democratic precincts and (2) exit poll discrepancies are highest where Bush voters predominated.**

4- **The Edison/Mitosky exit poll underscores a systematic bias in the official vote count. The corruption of the vote counting process overwhelmingly favored Bush: in 40 of the 50 states the exit polls showed Kerry winning but the vote count was fixed by the machines (not the voters) to favor Bush.**

5- **Given the above scientific evidence and the fact that Edison/Mitosky has refused to release all their raw exit poll data, the 2004 Presidential election merits a full investigation and exhaustive recount in the key swing states such as Florida and Ohio.**

The full US Count Votes report can be found at:
http://electionarchive.org/ucvAnalysis/US/Exit_Polls_2004_Edison-Mitofsky.pdf

The May 17, 2005 up-date can be found at:
http://uscountvotes.org/ucvAnalysis/US/exit-polls/USCV_exit_poll_simulations.pdf

An easy to read companion article, "A Corrupted Election: Despite what you may have heard, the exit polls were right" (Steve Freeman and Josh Mitteldorf, In These Times, February 15, 2005) can be found at:
http://www.inthesetimes.com/site/main/print/1970/

The results in New York State, which did not use electronic voting machines, demonstrate that Kerry beat Bush by a landside: 58 percent to 40 percent. People exaggerate by saying that New York is radically different from the other 49 states. The facts are that New York has a Republican Governor and rural New York is strongly Republican. If you want to compensate for New York's differences: cut the

18 percentage point difference in half or again into quarters—the result is still a landslide in favor of Kerry.

The vast majority of the voters had no confidence in the election process. Just prior to November's election, a CBS/NYT poll indicated that only 35% of registered voters had full confidence that their votes would be counted properly. That leaves around 100 million people who had only partial, little, or no confidence in America's election process.

Those who deny that the 2000 and 2004 elections were fixed are fooling themselves. The sad truth is that the people in the USA have come to accept and participate in what is "a culture of lies". The mass media promotes the "culture of lies" with false advertising, exaggerated "reality" shows, selling the Iraq War and covering its human horror up by hiding the massive destruction of civilian populations. We now live in George Orwell's 1984 where Big Brother (the Government and Corporate Media) tell the Big Lie. The story about the 2004 election fits this description.

PART II

HOW THE CORPORATE MEDIA SOLD US THE BUSH VICTORY

The mass media went far beyond brainwashing during the 2004 election. ABC, AP (Associated Press), CBS, CNN, Fox, and NBC created the National Election Pool (NEP) to provide tabulated vote counts and exit poll surveys. These organizations appointed Edison Media Research and Mitofsky International as the sole provider of exit polls. The AP collected the vote tallies.

The early CNN/Mitofsky exit polls indicated a Kerry victory in Florida, Ohio, and enough additional states to give Kerry a winning 300+ Electoral College total. The popular vote was projected to be a Kerry win with an exact reversal of Bush's "official" margin: 51%-48%. These projections of a Kerry win were duplicated by the final Zogby poll. Zogby International is a key polling organization.

On election night Kerry was ahead but by early morning Bush was ahead, representing a dramatic shift in the data base. The Exit Polls were contaminated by the Associated Press vote tallies which were fed to the networks. The AP purposely and knowingly mixed the election results from the manipulated electronic machines with the exit poll data (remember exit polls are NOT election results!) in the early hours of November 3, to "force" the exit polls to match the fraudulent election results. Of course, by "contaminating" the exit polls in this manner, they were NO LONGER exit polls but fraudulent results.

Both the New York Times and the MIT/Caltech election analysis team lied to the public by reporting that the earlier exit polls showing Kerry as the winner represented "too small a sample" and an "over-sampling" of Democrats to explain the change in the "exit polls" between 1 to 1:41 AM on November 3. They

have not apologized for this manipulation of public opinion based on unverified voting data and their bias against the possibility of election fraud.

This is the fundamental reason why the corporate media and press have imposed a news BLACKOUT on reporting election fraud: these companies have knowingly participated in the fraud process through the manipulation of election data. All the major media pronounced Bush the "winner". All have a vested interest in maintaining the myth of Bush's re-election! All used the same corrupted vote count data base.

The fundamental questions which the mass media refuses to answer, proving its complicity in fixing the 2004 election, are these:
1- Why was the raw Election Results data mixed with the Exit Poll data in the early hours of November 3? What purpose did this serve? How can it be justified?

2- Why was no step taken or question raised to audit the vote counting procedures and systems in order to find out why there was a discrepancy between the Exit Polls and the Election Results? What justified the assumption that the Exit Polls were wrong and the Election Results right?

3- Given these major discrepancies between Exit Polls and Results, as well as thousands of reports around the nation about voting anomalies, especially in Ohio, why was there a rush to declare Bush the winner without any further analysis?

4- Why has the Media (broadcast and written) been virtually silent on the events above; the Conyers Report http://truthout.org/Conyersreport.pdf.; **the fact that 31 members of the House of Representatives and Senator Barbara Boxer refused to certify Ohio's 20 electoral votes on January 6,2005; the manipulated recount in Ohio; and the major statistical reports which indicate that Kerry won?**

To determine who won the 2004 election all the votes in Ohio and Florida must be hand recounted. Of the 67 Florida counties, 52 used Optical Scan machines which have paper ballots which can be recounted. But 15 counties in the southern part of Florida used DREs, so there cannot be a recount. However, thousands of votes in these counties, including absentee votes were lost and not counted. Given these facts, *a special election in the 15 Florida DRE counties is justified and should be conducted on Optical Scan voting machines which produce paper trails that could be sampled after the vote to check the electronic outcome. THESE ARE THE MOST POPULOUS COUNTIES IN THE STATE OF FLORIDA.* Of the 88 counties in Ohio, only three (which were among the 10 most populous counties) used DREs. Therefore it is possible to recount the vast majority of Ohio's votes plus the 8,000 provisional ballots and the 93,000 "spoiled ballots" which had "no vote for president". If this is to be a real democracy, the votes must be recounted in Florida and Ohio!

PART III

WHAT IS TO BE DONE?

INVADE WASHINGTON, D.C. AND SET UP DEMOCRACY CITY

People need to take action. Otherwise they will die from depression and repression. By now it must be apparent what Bush represents:

1- **The elimination of Social Security.**
2- **The impoverishment of the middle classes.**
3- **The privatization of the public school system.**
4- **The transfer of wealth to the rich and super-rich.**
5- **Imperial wars to hold or capture oil reserves and markets.**
6- **The termination of labor unions and workers' pensions.**
7- **The destruction of any opposition through the use of "national security" mechanisms and laws to suppress dissent.**

Bush represents a Plutocratic, Corporatist State, which benefits the rich and cloaks itself in religious morality when, in fact, it is one of the most immoral governments which the USA has ever had. People in every Federal bureaucracy are forced to lie and participate in the manipulation of information. The campaign to privatize Social Security is but one example. Before that, there was false Medicare costs and the false reports about global warming put out by the EPA. The war on Iraq was based on lies.

Since oil reserves have "peaked", the USA, which is totally dependent on this source of energy, is now in the first stage of a major crisis. This crisis will be transformed into a "national security" issue. These Plutocrats plan to fix future elections. More DREs will be used in more states. A prime example of this was the removal of California Secretary of State, Kevin Shelley, the only secretary of state in the nation to stand up against the Diebold DREs. If there is any chance that the Plutocrats might loose the next presidential election, it may be postponed with a declaration of a "National Emergency" based on a real or fabricated terrorist attack. The Plutocrats need another ten years to fully remake U.S. society and hold down revolts from the masses. Keep in mind that key Bush operatives (John Negroponte; Elliot Abrams; Richard Armitage; Otto Reich; Colin Powell; plus hundreds of lower echelon operatives loyal to them and past CIA Director George Bush) led the Iran-Contra, extra-official government operation, *THE ENTERPRIZE*, against the will of Congress (e.g. the Boland Amendment). See
http://www.webcom.com/pinknoiz/covert/icsummary.html
http://www.counterpunch.com/mcgovern04272005.html
They lied to Congress and WE THE PEOPLE. They set up their own government. They defrauded the Constitution of the United States. How can anyone doubt that they stole two elections and will not attempt to impose their will no matter who dares to get in their way?

Stealing elections is one more manifestation of the character of the people who now rule the United States. In this sense, the argument for election fraud goes beyond mere statistics and points to the type of people who are willing to engage in this activity and approve its execution.

If the people wait to ride out Bush over the next four years, it will be too late. Our nation as we know it will have been destroyed. Now is the time to take action.

We must occupy Washington, D.C., as soon as possible and create a TENT CITY FOR DEMOCRACY. All the progressive organizations must coordinate and bring millions of people into D.C. to occupy it on a rotational basis. The major goal of this occupation will be to "de-legitimize" the Bush government so that it cannot implement its political program.

The call for mobilizing people to D.C. will be: COUNT THE VOTES IN OHIO AND FLORIDA. The major activities in the TENT CITY FOR DEMOCRACY will be "teach-ins" where experts will explain how the 2004 election was fixed. While we can expect that the U.S. mass media will not televise the "revolution", other, alternative media will, including the foreign press. This will further erode the credibility of the U.S. mass media, forcing it to cover the OCCUPATION.

It is quite possible that a "critical mass" of the population will demand a full recount of the vote in Ohio and Florida, including a new election in Florida's 15 DRE counties, but this time with Optical Scan machines. If this happens, Bush will be legitimately removed from government.

Another major goal in the TENT CITY FOR DEMOCRACY is to set up a CITIZENS COMMITTEE to write the new VOTING REFORM LAW.

This new Voting Reform Law should contain the following elements as recommended by US Count Votes http://uscountvotes.org/ucvAnalysis/US/exit-polls/USCV_exit_poll_simulations.pdf (pages 11-12):

"...
· full funding of the National Election Data Archive precinct level database.
· election equipment that permits access by non-specialist citizen election judges to recount voter verified paper ballots.
· routine 3%, randomly selected, independent audits of all elections.
· transparent and publicly accessible exit polling.
· election administration by non-partisan public civil servants.
· non-proprietary open-source coding for all computerized election equipment.
· no wired or wireless network connections to any vote casting or counting equipment.

Vote counts in America need to be routinely and independently audited. It is not enough to require voter verified paper records of ballots. These paper records must be easily and "independently"auditable by persons other than the voting machine vendor, preferably without having to hire computer technicians, paper roll advancers, bar code readers, and laptops, as is true with many voting systems on the market today.

In particular, 3% of randomly selected precincts can be recounted, using the paper record, immediately when polls close, in the precinct, before removing ballots from the precinct. If discrepancies are found, a county-wide recount can be automatically triggered. Additional funding may need to be allocated to state and county election offices to routinely perform independent audits of vote counts.

In order to audit their vote counts and monitor the accuracy of vote counting systems, all state and county election offices should set up election data reporting systems to quickly and easily make publicly available, their precinct-level vote totals, broken out by vote type (i.e. election day, absentee, overseas, provisional, early voting, etc.) If vote counts are not reported down to this detailed level, then padded votes in one vote type can easily "cancel out" under-votes in another type. In other words votes can be subtracted from one candidate in one vote type, while being added for another candidate in another vote type, yet these two problems, when added together, may look perfectly normal.

The Future: How would a National Election Data Archive Protect Democracy?

If, for decades, we had never independently audited our financial institutions, we would expect to see ubiquitous insider embezzlement of monies. For decades now, we have counted the vast majority of U.S. votes via mechanical or electronic methods, yet there have never been any routine independent audits of vote counts.
US Count Votes is seeking funding to create the first-ever nation-wide database of precinct-level and vote-type election results in order to statistically audit U.S. vote counts to detect patterns that suggest the embezzlement of votes. To obtain all the needed election data in all its diverse forms from the over 33,000 separate election offices in America is a huge project. Full-time programming staff, statisticians, and administrative staff are needed. For somewhat less than one million dollars, the National Election Data Archive could assist all candidates of any party to determine whether or not their elections were accurately counted, and produce court-worthy evidence that is needed to obtain recounts, investigations, or possibly even re-elections.

The "National Election Data Archive" project is particularly important, given the fact that private exit pollsters could, in the future, elect to adjust exit poll data to conform to actual official election results and neglect to publicly release any "unadjusted" exit poll data. The development of a "National Election Data Archive" would provide the public with all the data it needs to analyze vote counts within days of the November 2006 election. The technical implementation of well-developed and sound plans for such a system needs to begin very soon, in order to ensure by January 2007 and thereafter, that the candidates actually selected by the voters, are sworn into office. Our hope is that through careful analysis, we can develop the capacity to identify future vote count errors, whether fraudulent or inadvertent, in time to challenge the outcomes. "

THIS, MY FELLOW CITIZENS, IS WHAT MUST BE DONE. ANYTHING LESS WILL BRING GREATER SUFFERING TO ALL OF US AND THE WORLD.

VOTER FRAUD IN 2004: THE CASE OF PROPOSITION 66

19 FEBRUARY 2005

DAVID BAYER

Analysis of Proposition 66, Limitations on Three Strikes Law

One week before the November 2, 2004 election, the polls showed Proposition 66 passing by 66 percent to 34 percent:

State Totals:

For—5,604,060.....47.3 percent

Against—6,238,060.....52.7 percent.....lost by 634,000 votes.

In three Touch Screen Counties, the vote **against** was as follows:

Orange----------641,073.....62 percent

Riverside--------331,932.....61 percent

San Bernardino--322,981.....64 percent

Total 1,296,339 62 percent average.....10 percent above state average

These three counties produced more than two times the number of votes against Proposition 66 by which Proposition 66 lost: 1,296,339 versus 634,000. The "vote against" in each of these three counties was 10 percent above the state average.

THERE IS NO WAY FOR THESE THREE COUNTIES TO PROVE THAT PROPOSITION 66 LOST BY THE AMOUNTS RECORDED IN THESE COUNTIES.

THERE IS EVERY REASON IN THE WORLD—ESPECIALLY THE POLLS— TO DOUBT THESE RESULTS. THEY SHOULD BE CHALLENGED.

David Bayer
1912 Haussler Drive
Davis, CA 95616

Tel: 530-759-2004
email: bayer2@dcn.org

CALIFORNIA GOVERNOR RACE

MACHINE ANALYSIS FOR RECALL ELECTION OCTOBER 2003

EVIDENCE THAT THE ELECTION WAS FIXED

STATE RESULTS:

Cruz Bustamante (CB)= 32 %
Arnold Schwarzenegger (AS)= 49 %
Ratio AS / CB = 1.5

A- Mark Sense Ballot Card using Diebold- Accuvote OS machines:

County	CB %	AS %	Ratio AS/CB
1-Fresno	28	52	1.9
2-Humboldt	36	42	1.2
3-Kern	19	62	3.3
4-Lassen	15	61	4
5-Marin	48	32	.7
6-Modoc	14	61	4.4
7-Placer	17	63	3.7
8-San Joaquin	27	49	1.8
9-San Luis Obispo	26	50	1.9
10- Santa Barbara	31	47	1.5
11-Siskiyou	20	59	3
12-Trinity	22	53	2.4

13-Tulare	**23**	**56**	**2.4**
B- Touch Screen machines:			
1- Diebold Accu-Vote :			
14-Alameda	**54**	**26**	**.5**
15-Plumas	**20**	**55**	**2.8**
2- Sequoia Pacific AVC Edge:			
16-Riverside	**22**	**61**	**2.8**
17-Shasta	**17**	**58**	**3.4**
TOTAL			**41.7**

TOTAL MUST BE DIVIDED BY 17 TO GET AVERAGE = 2.5

ANALYSIS:
1- Schwarzenegger got 2.5 times as many votes as Bustamante from the DRE and Diebold machines on the average.

2- Schwarzenegger got 5/10 of as many votes as Bustamante from all the other non-DRE and non-Diebold machines used. That is, on the average, Bustamante beat Schwarzenegger on all the other machines.

$$\frac{.5\ S/B\ +\ 2.5\ S/B}{2} = 1.5\ S/B$$

where 1.5 is the State ratio of Schwarzenegger's votes to Bustamante's.

3- The DRE and Diebold machines produced the victory for Schwarzenegger, producing five times (5) as many votes for him relative to what the non-DREs produced for Bustamonte: 2.5 divided by .5 = 5 .

DRE= Direct Recording Electronic (paperless) voting machines. All the percentages come from the California Secretary of State Data Base.
http://www.wired.com/news/evote/0,2645,61947,00.html?tw=wn_polihead_6
17 counties used illegal Diebold software in the re-call election.

Bayer, David

From: Bayer, David [dbayer@saclink.csus.edu]
Sent: Wednesday, June 15, 2005 12:34 PM
To: bayer@csus.edu
Subject: Disenfranchisement: Putting Democracy at Risk with Paperless Voting Machines

Disenfranchisement: Putting Democracy at Risk with Paperless Voting Machines

David Bayer, October 2004

For several weeks California Secretary of State, Kevin Shelley, has come under attack for "playing politics" with the Help America Vote Act (HAVA) monies. This essay aims to demonstrate that Shelley's principal adversaries are led by the officers of the California Association of Clerks and Election Officials (CACEO) and that their prime motive for trying to bring Shelley down is due to his long standing effort to require that there be a paper ballot for each vote cast, no matter what type of voting machine may be used in an election. In this sense, contrary to the propaganda of the CACEO leadership, the California Secretary of State has defended the voting rights of millions of citizens in California and the rest of the United States. In a close election, when a recount is required, the paper ballot must be available. Without the ballots, there cannot be a recount.

Conny McCormack, Los Angeles County registrar; Stephen Weir, Contra Costa County registrar; Brad Clark, Alameda County registrar; and Scott Konopasek, San Bernardino County registrar have led the CACEO attack on Shelley. The first three are officers of CACEO, while Konopasek , along with McCormack, helped draft the 2002 HAVA legislation. The major flaw in HAVA was the fact that it did not require a paper ballot for each vote cast. The "no paper trail" flaw has been corrected with the implementation of the Federal Election Assistance Commission (EAC) in February 2004 and H.R. 3295, Section 301, which requires a paper record for every voting system beginning in January 2006. This is proof that the CACEO opposition to Shelley's call for a paper trail, first enunciated in a Press Release on November 21, 2003, was wrong and that Shelley was right: the vast majority of voters have no confidence in a voting system which is not backed up by a paper ballot.

While this may sound like the paper trail issue is resolved, it is not. In the up-coming November 2004 election some 50 million voters –one third of the electorate in the United States-will cast their ballots on paperless, touch screen electronic voting machines known as DREs (Direct Recording Electronic). Although Shelley began his battle against the DREs as early as April 2003, it was not until April 30, 2004, after holding months of hearings by the California Voting Systems and Procedures Panel, that he issued his "Decertification and Withdrawal of Approval of Certain DRE Voting Systems and Conditional Approval of the Use of Certain DRE Voting Systems". The Diebold DREs were permanently decertified while others were given a chance to meet 23 conditions to be certified for November 2004. The single most important condition was to have the DREs retrofitted to produce a paper ballot or for every voter to have the "option" of a paper ballot at the polling place using these machines. During the October 2003 Governor's recall election, and again in the March primary, Diebold used software in its DREs which was not approved by the Secretary of State. While Shelley's decertification of Diebold may secure the vote for millions of California citizens, the real problem is what is going to happen in the rest of the United States where Diebold DREs will be used extensively.

The tools and monies needed to avoid the 2000 Florida election fiasco have been too slow to come. HAVA was passed October 29, 2002. Bush appointed the commissioners to the EAC December 13, 2003. They made their first public presentation February 16, 2004. Their first hearings were held March 23, 2004. HAVA disbursed its first funds to the states in June 2004. Due to the fact that one third of the vote in the United States will be cast on machines without a paper trail, it is likely that more than half the population will not have confidence in the electoral process and that we shall have massive chaos in November which will dwarf Florida's fiasco.

Unfortunately, CACEO's President, Conny McCormack continues to lead the attack on Shelley and other citizens who want a more secure voting process as illustrated in her May 2004 testimony before the EAC: "Waving a 37-inch receipt that would be needed for each voter on a complicated ballot, Los Angeles election chief Conny B. McCormack said making voters pore over the cryptic printout with small type would guarantee confusion. "Touch screens have a proven track record of doing the best job," she said. "Voters are confident in these systems.

There's only a tiny, vocal minority making false claims to the contrary."

Such testimony is blatantly false. Konopasek who purchased $ 13.7 million of Sequoia DREs for San Bernardino; Clark who purchased $ 12.7 million of Diebold DREs; Weir; and McCormack have never done any educational campaign to inform citizens about computer security problems and voting machine alternatives. They have never conducted a county-wide survey in their respective areas to find out what the voters think about DREs.

The 75 year old League of United Latin American Citizens which represents millions of voters nationwide passed two 2004 resolutions calling for a paper ballot for each vote cast. The first LULAC resolution was passed at the California State Convention in Concord, May 21-23. The second LULAC resolution was approved at the National Convention held in San Antonio, Texas, July 6-10, by some 2,000 voting delegates. These resolutions are much more powerful evidence than arbitrary declarations by CACEO officials that a significant sector of the U.S. electorate wants a paper trail at the polls. Citizens have read about or experienced hundreds of computer system failures during elections. Moreover, the vast majority of computer experts have testified that the systems can either be hacked or fail during the tabulation of votes.

An October 2004 Field Poll found that only 23 percent of California voters felt "very confident" about touch-screen machines. Such numbers are one reason federal law requires all counties to provide a "voter verifiable paper trail" by 2006.

Thanks to Shelley, voters nationwide have become aware of potential electoral fraud. Had the 2003 requests of the California Secretary of State for a paper trail been heeded, the coming November elections would inspire far more confidence in the electoral results than we are likely to observe.

Those who fought for clean elections achieved a major victory. For the first time since 1877, the Electoral College votes were challenged. Thirtyone House members supported the Decertification of Ohio's 20 electoral votes while one brave Senator, Barbara Boxer, voted for Decertification. The vote for certification in the Republican controlled Congress was 267 in the House and 74 in the Senate. We salute those brave Democrats who voted to preserve our democracy
http://clerk.house.gov/evs/2005/roll007.xml .

The structural defect in our Constitution which permits members of Congress to be sworn in two days before voting on Electoral College certification (January 6) explains why most will not question the electoral votes. An "inherent conflict of interest" exists: if the President and Vice President were elected through fraud, it is likely that many Congress people were so elected (e.g. Martinez in Florida).

The Report by Congressman Conyers documents fraud in Ohio. Fraud took place in many states. Florida was the most notorious where the election was controlled by Bush's brother, Governor Jeb Bush, and the Republican Secretary of State, Glenda Hood, who played the same roll as Ohio's Secretary of State, Kenneth Blackwell, disenfranchising millions of voters and perpetuating the November 2004 electoral fraud.http://www.truthout.org/Conyersreport.pdf.

Contrary to Congressional ignorance (even those who objected to Ohio's electoral votes) if a full hand recount was conducted in Ohio and Florida, Kerry would carry both states as the Exit Polls predicted. Kerry won the popular vote as well as the electoral vote.
http://freepress.org/images/departments/PopularVotePaper181_1.pdf and
http://www.buzzflash.com/alerts/04/11/The_unexplained_exit_poll_discrepancy_v00k.pdf .

The real question for those who dismiss fraud is: Why are Bush people afraid to conduct a full hand recount in Ohio and Florida?

The only method to prove that Bush won the November 2004 election is to recount the votes in Florida and Ohio. **WITHOUT THE RECOUNT, BUSH, ONCE AGAIN, AS IN 2000, HAS BEEN ILLEGITAMATELY ELECTED PRESIDENT .**

The argument for new elections in Kiev was the discrepancy between exit polls and voting results. Ironically, in the United States where massive fraud is documented (Exit Polls; the Kathy Dopp study of Florida's 52 optical scan counties where 500,000 votes transferred from Kerry to Bush; the UC Berkeley study of Florida's 15 Touch Screen counties where 130,000 to 260,000 votes went from Kerry to Bush; the Miami Herald recount in Florida projecting another 400,000 votes for Kerry, thereby beating Bush who led by 381,000 votes;and Conyer's Report on Ohio where 93,000 spoiled ballots had no vote for President, 8,000 provisional ballots were thrown out and hundreds of other irregularities add Kerry votes surpassing Bush's 119,000 margin) there is no demand for recounts or new elections in Florida and Ohio. People in Kiev love democracy more than people in the United States? Or is the **SILENCE** of Propaganda Media powerful enough to destroy our democracy?

Bayer, David

From: David Bayer [bayer2@dcn.org]
Sent: Sunday, January 02, 2005 1:59 AM
To: Undisclosed-Recipient:@csus.edu;
Subject: Getting Ready for the Next Fixed Election: the New York Times

Amigos:

The problem with allowing the Republicans to get away with another stolen election is that they shall institutionalize the system of having "private companies manage fixed elections" ; the judges which they appoint to the Court system will uphold or "reconstruct" the legal system so that these "fixed" elections will be legal; and the Media concentration (a non-free press in fewer and fewer hands) will guarantee that the people will KNOW NOTHING.

So if that is what you want, that is what you will get by allowing it to happen: **NO MORE DEMOCRACY .**

This is the minimum needed to break the power of a small ruling class driving 90 percent of the rest of the U.S. population into Third World status:

1- electronic voting should be prohibited, optical scan or touch screen, both can be manipulated and intervened.

2- if electronic machines are used, these should be the requirements:

2.1- a paper ballots for each vote cast, locked in boxes and saved for a recount.

2.2- obligatory recounts based on sampling the votes in each precinct to make sure that each electronic total in each precinct matches the sample drawn. We are NOT interested in how close the vote is or if there was a landslide for one candidate or issue (e.g. Proposition X). OBLIGATORY RECOUNT MEANS EXACTLY WHAT IT SAYS: a random sample of the paper ballots must be drawn to check its results with the electronic results at each precint!

The 2.2 requirement is a new requirement. Call it the Bayer requirement, if you like. But remember it. If NOT DONE, the process is open to fraud.

3- Polls: Pre-voting polls (three days before the election) and Exit Polls are additional guarantees of voting integrity (read: preventing fraud). In fact, Exit Polls are the most important mechanism for preventing fraud whether or not electronic voting technologies have been used.

Exit polls should be required to be executed by every Secretary of State. Other entities can do them. But there is NO EXCUSE for these not being done by the States.

4- The entire voting system must be in public hands. There should be NO private enterprise participation in the voting process. The Secretary of State position in each state of the union should be NON-PARTISON.

5- Elections should be publicly financed and there should be equal time in the Media for all candidates.

david bayer
2 january 05

December 27, 2004

MAKING VOTES COUNT

Setting Standards for Fair Elections

The much-delayed work of setting federal standards for electronic voting machines is speeding up, and there is reason for concern. Voting machine companies and their supporters have been given a large say in the process, while advocates for voters, including those who insist on the use of voter-verified paper receipts, have been pushed to the margins. Election officials and machine makers may be betting that after the presidential election, ordinary Americans have lost interest in the mechanics of the ballot. But Americans do care, and it is unlikely that they will be satisfied by a process in which special interests dominate, or by a result that does not ensure vote totals that can be trusted.

The No. 1 goal of the new standards should be ensuring that the machines will not, by accident or design, produce false vote totals. It is increasingly clear that voters want electronic, A.T.M.-type voting machines that produce verifiable paper records, or other systems like optical scan machines, where votes are cast on paper as a check on the reliability of machines. California, Ohio and other states require paper trails by law, and New York appears poised to join them.

The Election Assistance Commission, a federal body set up after the 2000 election mess, has created a group called the Technical Guidelines Development Committee to propose federal electronic voting standards to Congress this spring. This committee includes outspoken supporters of electronic voting without paper trails, including Britain Williams, a retired Kennesaw State University professor who has worked closely with Georgia on its controversial adoption of Diebold voting machines. But disappointingly, the commission did not include any of the many respected computer scientists - such as Prof. Aviel Rubin of Johns Hopkins, Prof. David Dill of Stanford or Dr. Rebecca Mercuri - who have been warning about the unreliability of electronic voting in its current form.

The election commission is expected to rely heavily on standards being developed by a nonprofit association of engineers, computer scientists and other professionals with the unfortunate acronym of I.E.E.E., which develops technical standards for such things as wireless communications. But the voting machine industry plays a disconcertingly large role in this organization. The chairman of the working group preparing the standards for voting machines is a top executive of Election Systems and Software, a large and controversial voting machine maker. The head of the committee that oversees the working group has a seat on the election commission's voting machines standards committee. He is a consultant who has been hired in the past by companies in the elections field. Because of the insular nature of the engineering panel's meetings, ordinary voters - who have an important stake - have had little chance to participate. Over the objections of some members of the working group, the current draft of the election-machine standards merely makes voter-verified paper trails optional. The draft's scope is also too narrow: it fails to address many ways in which vote totals could be rigged.

The Election Assistance Commission has a chance to lead the nation to a new generation of technology that voters can trust. But if it fails, there are other routes. California has developed its own state standards for machines with paper trails, and other states could do likewise. And some of the nation's leading election reform advocates, election officials and voting machine makers are forming a new group, called Voting System Performance Rating, that hopes to develop standards in a more inclusive way. Whoever sets the standards, the process and the result need to give voters complete confidence that their votes will be accurately counted.

Bayer, David

From: Bayer, David [dbayer@saclink.csus.edu]

Sent: Wednesday, June 15, 2005 12:28 PM

To: bayer@csus.edu

Subject: Executive Summary of Conyers Report to Congress about Electoral Fraud in Ohio 6 Jan 05 and Sample Letter

Preserving Democracy:
What Went Wrong in Ohio
Status Report of the House Judiciary Committee Democratic Staff

Wednesday 05 January 2005

Executive Summary

Representative John Conyers, Jr., the Ranking Democrat on the House Judiciary Committee, asked the Democratic staff to conduct an investigation into irregularities reported in the Ohio presidential election and to prepare a Status Report concerning the same prior to the Joint Meeting of Congress scheduled for January 6, 2005, to receive and consider the votes of the electoral college for president. The following Report includes a brief chronology of the events; summarizes the relevant background law; provides detailed findings (including factual findings and legal analysis); and describes various recommendations for acting on this Report going forward.

We have found numerous, serious election irregularities in the Ohio presidential election, which resulted in a significant disenfranchisement of voters. Cumulatively, these irregularities, which affected hundreds of thousand of votes and voters in Ohio, raise grave doubts regarding whether it can be said the Ohio electors selected on December 13, 2004, were chosen in a manner that conforms to Ohio law, let alone federal requirements and constitutional standards.

This report, therefore, makes three recommendations: (1) consistent with the requirements of the United States Constitution concerning the counting of electoral votes by Congress and Federal law implementing these requirements, there are ample grounds for challenging the electors from the State of Ohio; (2) Congress should engage in further hearings into the widespread irregularities reported in Ohio; we believe the problems are serious enough to warrant the appointment of a joint select Committee of the House and Senate to investigate and report back to the Members; and (3) Congress needs to enact election reform to restore our people's trust in our democracy. These changes should include putting in place more specific federal protections for federal elections, particularly in the areas of audit capability for electronic voting machines and casting and counting of provisional ballots, as well as other needed changes to federal and state election laws.

With regards to our factual finding, in brief, we find that there were massive and unprecedented voter irregularities and anomalies in Ohio. In many cases these irregularities were caused by intentional misconduct and illegal behavior, much of it involving Secretary of State J. Kenneth Blackwell, the co-chair of the Bush-Cheney campaign in Ohio.

First, in the run up to election day, the following actions by Mr. Blackwell, the Republican Party and election officials disenfranchised hundreds of thousands of Ohio citizens, predominantly minority and Democratic voters:

- **The misallocation of voting machines led to unprecedented long lines that disenfranchised scores, if not hundreds of thousands, of predominantly minority and Democratic voters.** This was illustrated by the fact that the Washington Post reported that in Franklin County, "27 of the 30 wards with the most machines per registered voter showed majorities for Bush. At the other end of the spectrum, six of the seven wards with the fewest machines delivered large margins for Kerry." *(See Powell and Slevin, supra)*. Among other things, the conscious failure to provide sufficient voting machinery violates the Ohio Revised Code which requires the Boards of Elections to "provide adequate facilities at each polling place for conducting the election."
- **Mr. Blackwell's decision to restrict provisional ballots resulted in the disenfranchisement of tens, if not hundreds, of thousands of voters, again predominantly minority and Democratic voters.** Mr. Blackwell's decision departed from past Ohio law on provisional ballots, and there is no evidence that a broader construction would have led to any significant disruption at the polling places, and did not do so in other states.
- **Mr. Blackwell's widely reviled decision to reject voter registration applications based on paper weight may have resulted in thousands of new voters not being registered in time for the 2004 election.**
- **The Ohio Republican Party's decision to engage in preelection "caging" tactics, selectively targeting 35,000 predominantly minority voters for intimidation had a negative impact on voter turnout.** The Third Circuit found these activities to be illegal and in direct violation of consent decrees barring the Republican Party from targeting minority voters for poll challenges.
- **The Ohio Republican Party's decision to utilize thousands of partisan challengers concentrated in minority and Democratic areas likely disenfranchised tens of thousands of legal voters, who were not only intimidated, but became**

discouraged by the long lines. Shockingly, these disruptions were publicly predicted and acknowledged by Republican officials: Mark Weaver, a lawyer for the Ohio Republican Party, admitted the challenges "can't help but create chaos, longer lines and frustration."

- **Mr. Blackwell's decision to prevent voters who requested absentee ballots but did not receive them on a timely basis from being able to receive provisional ballots 6 likely disenfranchised thousands, if not tens of thousands, of voters, particularly seniors.** A federal court found Mr. Blackwell's order to be illegal and in violation of HAVA.

Second, on election day, there were numerous unexplained anomalies and irregularities involving hundreds of thousands of votes that have yet to be accounted for:

- **There were widespread instances of intimidation and misinformation in violation of the Voting Rights Act, the Civil Rights Act of 1968, Equal Protection, Due Process and the Ohio right to vote.** Mr. Blackwell's apparent failure to institute a single investigation into these many serious allegations represents a violation of his statutory duty under Ohio law to investigate election irregularities.
- **We learned of improper purging and other registration errors by election officials that likely disenfranchised tens of thousands of voters statewide.** The Greater Cleveland Voter Registration Coalition projects that in Cuyahoga County alone over 10,000 Ohio citizens lost their right to vote as a result of official registration errors.
- **There were 93,000 spoiled ballots where no vote was cast for president, the vast majority of which have yet to be inspected.** The problem was particularly acute in two precincts in Montgomery County which had an undervote rate of over 25% each - accounting for nearly 6,000 voters who stood in line to vote, but purportedly declined to vote for president.
- **There were numerous, significant unexplained irregularities in other counties throughout the state:** (i) In Mahoning county at least 25 electronic machines transferred an unknown number of Kerry votes to the Bush column; (ii) Warren County locked out public observers from vote counting citing an FBI warning about a potential terrorist threat, yet the FBI states that it issued no such warning; (iii) the voting records of Perry county show significantly more votes than voters in some precincts, significantly less ballots than voters in other precincts, and voters casting more than one ballot; (iv) in Butler county a down ballot and underfunded Democratic State Supreme Court candidate implausibly received more votes than the best funded Democratic Presidential candidate in history; (v) in Cuyahoga county, poll worker error may have led to little known thirdparty candidates receiving twenty times more votes than such candidates had ever received in otherwise reliably Democratic leaning areas; (vi) in Miami county, voter turnout was an improbable and highly suspect 98.55 percent, and after 100 percent of the precincts were reported, an additional 19,000 extra votes were recorded for President Bush.

Third, in the post-election period we learned of numerous irregularities in tallying provisional ballots and conducting and completing the recount that disenfanchised thousands of voters and call the entire recount procedure into question (as of this date the recount is still not complete):

- **Mr. Blackwell's failure to articulate clear and consistent standards for the counting of provisional ballots resulted in the loss of thousands of predominantly minority votes.** In Cuyahoga County alone, the lack of guidance and the ultimate narrow and arbitrary review standards significantly contributed to the fact that 8,099 out of 24,472 provisional ballots were ruled invalid, the highest proportion in the state.
- ***Mr. Blackwell's failure to issue specific standards for the recount contributed to a lack of uniformity in violation of both the Due Process Clause and the Equal Protection Clauses.*** We found innumerable irregularities in the recount in violation of Ohio law, including (i) counties which did not randomly select the precinct samples; (ii) counties which did not conduct a full hand court after the 3% hand and machine counts did not match; (iii) counties which allowed for irregular marking of ballots and failed to secure and store ballots and machinery; and (iv) counties which prevented witnesses for candidates from observing the various aspects of the recount.
- **The voting computer company Triad has essentially admitted that it engaged in a course of behavior during the recount in numerous counties to provide "cheat sheets" to those counting the ballots.** The cheat sheets informed election officials how many votes they should find for each candidate, and how many over and under votes they should calculate to match the machine count. In that way, they could avoid doing a full county-wide hand recount mandated by state law.

Download Full PDF Document
Size: 3.22 MB
102 Pages

Get Adobe Reader
Requires Adobe Reader

Eve Roberson to CA Voting Systems & Procedures Panel Hearing 6/16/05 on Costs

.

Mr. Chairman and members of the Panel,

I'm Eve Roberson of Santa Rosa, CA. As a retired election supervisor I am intimately aware of the many details that go into a successful election. I think we can all agree that to have a successful election the voters must, above all else, be assured that their votes are accurately counted.

In order to have votes counted accurately we must have electronic equipment that cannot be hacked. Unfortunately, neither of the two systems under consideration today can assure voters of that, as demonstrated in past elections in which they have been used.

I support the spirit of the Help America Vote Act (HAVA) and I do not want the State to squander our hundreds of millions of taxpayer dollars on any equipment which does not meet open and secure election standards and which will have to be replaced within a few years, as technology changes.

But I am concerned not only with the huge initial costs of this complex equipment which makes our HAVA funding only a down payment. Their hidden costs then become just one more unfunded mandate: Storage, transportation, repair and maintenance, personnel costs, special training, constant battery charging and roving teams of technicians, to name a few.

The technology is not proven yet. So until electronic voting systems that provide transparency and auditability are available, paper ballots, optically scanned, will continue to provide Californians with secure elections. This is an accurate, low cost alternative to the costly and risky voting systems of Diebold and ES&S. Handicap access can be met with simple add-on audio and tactile assistance devices.

We owe our citizens the assurance that their votes will be accurately counted. Our democracy depends upon it. It is for these reasons I urge you today to reject Diebold and ES&S voting systems for use in our State.

Thank you.

Bayer, David

From: Bayer, David [dbayer@saclink.csus.edu]
Sent: Wednesday, June 15, 2005 12:28 PM
To: bayer@csus.edu
Subject: Executive Summary of Conyers Report to Congress about Electoral Fraud in Ohio 6 Jan 05 and Sample Letter

Preserving Democracy:
What Went Wrong in Ohio
Status Report of the House Judiciary Committee Democratic Staff

Wednesday 05 January 2005

Executive Summary

Representative John Conyers, Jr., the Ranking Democrat on the House Judiciary Committee, asked the Democratic staff to conduct an investigation into irregularities reported in the Ohio presidential election and to prepare a Status Report concerning the same prior to the Joint Meeting of Congress scheduled for January 6, 2005, to receive and consider the votes of the electoral college for president. The following Report includes a brief chronology of the events; summarizes the relevant background law; provides detailed findings (including factual findings and legal analysis); and describes various recommendations for acting on this Report going forward.

We have found numerous, serious election irregularities in the Ohio presidential election, which resulted in a significant disenfranchisement of voters. Cumulatively, these irregularities, which affected hundreds of thousand of votes and voters in Ohio, raise grave doubts regarding whether it can be said the Ohio electors selected on December 13, 2004, were chosen in a manner that conforms to Ohio law, let alone federal requirements and constitutional standards.

This report, therefore, makes three recommendations: (1) consistent with the requirements of the United States Constitution concerning the counting of electoral votes by Congress and Federal law implementing these requirements, there are ample grounds for challenging the electors from the State of Ohio; (2) Congress should engage in further hearings into the widespread irregularities reported in Ohio; we believe the problems are serious enough to warrant the appointment of a joint select Committee of the House and Senate to investigate and report back to the Members; and (3) Congress needs to enact election reform to restore our people's trust in our democracy. These changes should include putting in place more specific federal protections for federal elections, particularly in the areas of audit capability for electronic voting machines and casting and counting of provisional ballots, as well as other needed changes to federal and state election laws.

With regards to our factual finding, in brief, we find that there were massive and unprecedented voter irregularities and anomalies in Ohio. In many cases these irregularities were caused by intentional misconduct and illegal behavior, much of it involving Secretary of State J. Kenneth Blackwell, the co-chair of the Bush-Cheney campaign in Ohio.

First, in the run up to election day, the following actions by Mr. Blackwell, the Republican Party and election officials disenfranchised hundreds of thousands of Ohio citizens, predominantly minority and Democratic voters:

- **The misallocation of voting machines led to unprecedented long lines that disenfranchised scores, if not hundreds of thousands, of predominantly minority and Democratic voters.** This was illustrated by the fact that the Washington Post reported that in Franklin County, "27 of the 30 wards with the most machines per registered voter showed majorities for Bush. At the other end of the spectrum, six of the seven wards with the fewest machines delivered large margins for Kerry." *(See Powell and Slevin, supra).* Among other things, the conscious failure to provide sufficient voting machinery violates the Ohio Revised Code which requires the Boards of Elections to "provide adequate facilities at each polling place for conducting the election."
- **Mr. Blackwell's decision to restrict provisional ballots resulted in the disenfranchisement of tens, if not hundreds, of thousands of voters, again predominantly minority and Democratic voters.** Mr. Blackwell's decision departed from past Ohio law on provisional ballots, and there is no evidence that a broader construction would have led to any significant disruption at the polling places, and did not do so in other states.
- **Mr. Blackwell's widely reviled decision to reject voter registration applications based on paper weight may have resulted in thousands of new voters not being registered in time for the 2004 election.**
- **The Ohio Republican Party's decision to engage in preelection "caging" tactics, selectively targeting 35,000 predominantly minority voters for intimidation had a negative impact on voter turnout.** The Third Circuit found these activities to be illegal and in direct violation of consent decrees barring the Republican Party from targeting minority voters for poll challenges.
- **The Ohio Republican Party's decision to utilize thousands of partisan challengers concentrated in minority and Democratic areas likely disenfranchised tens of thousands of legal voters, who were not only intimidated, but became**

discouraged by the long lines. Shockingly, these disruptions were publicly predicted and acknowledged by Republican officials: Mark Weaver, a lawyer for the Ohio Republican Party, admitted the challenges "can't help but create chaos, longer lines and frustration."

- **Mr. Blackwell's decision to prevent voters who requested absentee ballots but did not receive them on a timely basis from being able to receive provisional ballots 6 likely disenfranchised thousands, if not tens of thousands, of voters, particularly seniors.** A federal court found Mr. Blackwell's order to be illegal and in violation of HAVA.

Second, on election day, there were numerous unexplained anomalies and irregularities involving hundreds of thousands of votes that have yet to be accounted for:

- **There were widespread instances of intimidation and misinformation in violation of the Voting Rights Act, the Civil Rights Act of 1968, Equal Protection, Due Process and the Ohio right to vote.** Mr. Blackwell's apparent failure to institute a single investigation into these many serious allegations represents a violation of his statutory duty under Ohio law to investigate election irregularities.
- **We learned of improper purging and other registration errors by election officials that likely disenfranchised tens of thousands of voters statewide.** The Greater Cleveland Voter Registration Coalition projects that in Cuyahoga County alone over 10,000 Ohio citizens lost their right to vote as a result of official registration errors.
- **There were 93,000 spoiled ballots where no vote was cast for president, the vast majority of which have yet to be inspected.** The problem was particularly acute in two precincts in Montgomery County which had an undervote rate of over 25% each - accounting for nearly 6,000 voters who stood in line to vote, but purportedly declined to vote for president.
- **There were numerous, significant unexplained irregularities in other counties throughout the state:** (i) in Mahoning county at least 25 electronic machines transferred an unknown number of Kerry votes to the Bush column; (ii) Warren County locked out public observers from vote counting citing an FBI warning about a potential terrorist threat, yet the FBI states that it issued no such warning; (iii) the voting records of Perry county show significantly more votes than voters in some precincts, significantly less ballots than voters in other precincts, and voters casting more than one ballot; (iv) in Butler county a down ballot and underfunded Democratic State Supreme Court candidate implausibly received more votes than the best funded Democratic Presidential candidate in history; (v) in Cuyahoga county, poll worker error may have led to little known thirdparty candidates receiving twenty times more votes than such candidates had ever received in otherwise reliably Democratic leaning areas; (vi) in Miami county, voter turnout was an improbable and highly suspect 98.55 percent, and after 100 percent of the precincts were reported, an additional 19,000 extra votes were recorded for President Bush.

Third, in the post-election period we learned of numerous irregularities in tallying provisional ballots and conducting and completing the recount that disenfanchised thousands of voters and call the entire recount procedure into question (as of this date the recount is still not complete):

- **Mr. Blackwell's failure to articulate clear and consistent standards for the counting of provisional ballots resulted in the loss of thousands of predominantly minority votes.** In Cuyahoga County alone, the lack of guidance and the ultimate narrow and arbitrary review standards significantly contributed to the fact that 8,099 out of 24,472 provisional ballots were ruled invalid, the highest proportion in the state.
- ***Mr. Blackwell's failure to issue specific standards for the recount contributed to a lack of uniformity in violation of both the Due Process Clause and the Equal Protection Clauses.*** We found innumerable irregularities in the recount in violation of Ohio law, including (i) counties which did not randomly select the precinct samples; (ii) counties which did not conduct a full hand court after the 3% hand and machine counts did not match; (iii) counties which allowed for irregular marking of ballots and failed to secure and store ballots and machinery; and (iv) counties which prevented witnesses for candidates from observing the various aspects of the recount.
- **The voting computer company Triad has essentially admitted that it engaged in a course of behavior during the recount in numerous counties to provide "cheat sheets" to those counting the ballots.** The cheat sheets informed election officials how many votes they should find for each candidate, and how many over and under votes they should calculate to match the machine count. In that way, they could avoid doing a full county-wide hand recount mandated by state law.

Those who fought for clean elections achieved a major victory. For the first time since 1877, the Electoral College votes were challenged. Thirtyone House members supported the Decertification of Ohio's 20 electoral votes while one brave Senator, Barbara Boxer, voted for Decertification. The vote for certification in the Republican controlled Congress was 267 in the House and 74 in the Senate. We salute those brave Democrats who voted to preserve our democracy
http://clerk.house.gov/evs/2005/roll007.xml .

The structural defect in our Constitution which permits members of Congress to be sworn in two days before voting on Electoral College certification (January 6) explains why most will not question the electoral votes. An "inherent conflict of interest" exists: if the President and Vice President were elected through fraud, it is likely that many Congress people were so elected (e.g. Martinez in Florida).

The Report by Congressman Conyers documents fraud in Ohio. Fraud took place in many states. Florida was the most notorious where the election was controlled by Bush's brother, Governor Jeb Bush, and the Republican Secretary of State, Glenda Hood, who played the same roll as Ohio's Secretary of State, Kenneth Blackwell, disenfranchising millions of voters and perpetuating the November 2004 electoral fraud.http://www.truthout.org/Conyersreport.pdf.

Contrary to Congressional ignorance (even those who objected to Ohio's electoral votes) if a full hand recount was conducted in Ohio and Florida, Kerry would carry both states as the Exit Polls predicted. Kerry won the popular vote as well as the electoral vote.
http://freepress.org/images/departments/PopularVotePaper181_1.pdf and
http://www.buzzflash.com/alerts/04/11/The_unexplained_exit_poll_discrepancy_v00k.pdf .

The real question for those who dismiss fraud is: Why are Bush people afraid to conduct a full hand recount in Ohio and Florida?

The only method to prove that Bush won the November 2004 election is to recount the votes in Florida and Ohio. **WITHOUT THE RECOUNT, BUSH, ONCE AGAIN, AS IN 2000, HAS BEEN ILLEGITAMATELY ELECTED PRESIDENT .**

The argument for new elections in Kiev was the discrepancy between exit polls and voting results. Ironically, in the United States where massive fraud is documented (Exit Polls; the Kathy Dopp study of Florida's 52 optical scan counties where 500,000 votes transferred from Kerry to Bush; the UC Berkeley study of Florida's 15 Touch Screen counties where 130,000 to 260,000 votes went from Kerry to Bush; the Miami Herald recount in Florida projecting another 400,000 votes for Kerry, thereby beating Bush who led by 381,000 votes;and Conyer's Report on Ohio where 93,000 spoiled ballots had no vote for President, 8,000 provisional ballots were thrown out and hundreds of other irregularities add Kerry votes surpassing Bush's 119,000 margin) there is no demand for recounts or new elections in Florida and Ohio. People in Kiev love democracy more than people in the United States? Or is the **SILENCE** of Propaganda Media powerful enough to destroy our democracy?

Bayer, David

From: David Bayer [bayer2@dcn.org]
Sent: Thursday, February 10, 2005 10:58 PM
To: Undisclosed-Recipient:@csus.edu;
Subject: Questions the Media and Bush People Will Not Answer Because They Prove the Election Was Fixed

Thursday, 3 February 2005, 11:20 am
Opinion: Ernest Partridge

***"Shut Up!,"* They Explain**

"'Buzz Off' in no way constitutes valid rebuttal." –New Yorker Cartoon
(From memory)

Have you noticed?

Those of us who suspect that the election was stolen (a.k.a. "conspiracy nuts"), have presented an impressive array of evidence – statistical, anecdotal and circumstantial – to support our claims. In response to this we have been provided scant rebuttal evidence.

Instead, we have been ridiculed, vilified, and, most damaging of all, ignored. If our concerns are warranted, then the manipulation of the past election (and perhaps the elections of 2000 and 2002 as well) is arguably the most important news event since the founding of our republic, for a fraudulent national election strikes at the very heart of our democracy. If we the people of the United States are no longer able to remove the government through the ballot box, we are no longer ruled "with the consent of the governed." Government of, by, and for the people is finished.

Furthermore, "the press" (which we now call "the media") is no longer our defense against tyranny, for it now serves the government. To be sure, the conventional view that George Bush and the Republicans won the election "fair and square," is not without a few defenses. But, as I attempted to demonstrate in my previous essay (" Has the Case for Election Fraud been Refuted "), these arguments do not stand up to close inspection. And what, for the most part, is the response when the skeptics confront the media and the "winners" with their questions and their evidence, and demand an explanation?

"Shut Up!," they explain.

In this essay, I will take a different approach to the issue of electoral integrity. Rather than continue with accusations and evidence, both new and re-iterated, I will pose a series of questions – questions which, for the most part, have been ignored by the media and by the beneficiaries of the past election, the Bush Administration and the Republican Party.

It is far better that we ask questions about the integrity of our elections than make accusations. Accusations soon become tedious and wear out their welcome. But questions put our adversaries on the defensive – which is where they most assuredly belong.

These are questions about the last three elections that must not be allowed to fade away. Not unless and until they are plausibly answered. And if they are not plausibly answered, then decisive action by the American citizens is very much in order. These questions have not been answered, and there is little evidence so far that

they ever will be.

"Shut Up!" "Get over it!" "Let's move on!" Are not answers.

Now to the questions:

Can the GOP provide proof that the paperless voting machines and the compiling computers (manufactured and coded by Republicans) provided accurate tallies of the voting? Could they do so if they wanted to? If not, why not?

Clearly the Republicans can provide no such proof directly, because the machines were deliberately designed not to provide such proof – there are no paper records, and the source code (software) is secret. Thus, in response to the demand for validation, the manufacturers have only one possible response: *"Trust us!"*

Of course, voting results could be audited and validated if it were required by law. In fact, validation is required in the state of Nevada, and thus, in that state at least, e-voting machines produce paper records of each vote.

Even without paper records, indirect methods of validation can be devised. For example, a sampling of e-voting machines could be selected at random during election day, "pulled" from the precincts, and checked for input/output consistency. Another method would be a random selection of polling precincts where voters would be asked to vote first with e-voting machines and then again with paper ballots. (Only one vote per voter would officially count, of course). If the machines were "fixed," this would show up in a comparison of the totals. (For more detail, see my blog of October 30, 2004). With both of these cases, of course, the selection of test machines must be totally random and performed during election day. No such validation procedures were performed anywhere during the November 2, election.

Absent paper records and election day verification procedures, there remain statistical analyses. As I have argued elsewhere (here ,here , and here), these studies indicate compelling evidence of fraud. Predictably, they have been almost totally ignored by the mainstream media.

Why won't the e-voting machines provide auditable paper records?

I've heard two answers to this question, both laughably inadequate: (a) paper records would be prohibitively expensive, and (b) paper records would be impossibly impractical. Both excuses have been decisively refuted by perfectly affordable and practical use of paper validation in the state of Nevada. In addition, Diebold Corp., one of the two largest manufacturers of e-voting machines, also makes ATM machines and the credit card mechanisms on gasoline pumps. Both, of course, produce paper records. So why not also for e-voting machines?

A few months ago, I happened to see on CSPAN a hearing by the Federal Election Commission on the e-voting machines. When asked if paper records would be feasible, one witness produced a printout that was several feet long, and proclaimed that such a printout would be required for every vote. This of course was a damnable lie, clearly exposed, once again, by the employment of paper validation in Nevada. That "demonstration" before the Commission can only be interpreted as evidence of the desperation of those who doggedly oppose (for whatever covert reasons) the use of paper records of e-voting.

Why won't the Diebold and ES&S corporations publish their source codes?

The standard answer is these codes are the private ("proprietary") property of the corporations, and thus must be kept secret to protect that property. Kinda like Col. Sanders' recipe for Kentucky Fried Chicken.

But there are patent and copyright laws to protect "intellectual property." Moreover, most of the "property"

protected by copyright, namely musical and literary works, are by their very nature, public entities – i.e., not "secret." So if songs and novels and essays and movies can all be protected by copyrights, why not the source codes for e-voting and vote compiling machines? The insistence by the voting code writers that these codes most nonetheless be kept secret, can only lead one to wonder: "just what are they trying to hide?"

If Diebold, ES&S, etc. have, as they contend, nothing to hide, why do they continue to compromise their reputations by refusing to release the codes for public inspection?

The computerized compiling of regional (e.g., statewide) returns provides another opportunity for election fraud. Is it possible to ensure the accuracy of the compiling process and to defeat attempts to "rig" these totals through computer hacking? If so, are such verification methods in use? If not, then why not?

It is, in fact, possible to ensure the accuracy of compiled election returns. One strategy would be to utilize two independent parallel compiling methods and teams. If the resulting totals are identical, there is very little chance of fraud. If there is a significant disparity in the results, then a recount by yet another method should be initiated automatically. I am not aware that such validation procedures were operating in the last elections. So, to summarize the answers to this three-part question: Yes, it is possible to check and ensure the accuracy of statewide compilations. No, it appears that these verification methods are not in use. The third part – "if not, why not?" – is for the defenders of the present system to answer.

Our remaining questions stand alone, and require no commentary.

1. *Congressman Rush Holt (D. NJ) and Senator Hillary Clinton (D. NY) both introduced bills that would require paper records of votes cast on e-voting machines. Both bills were killed in the House and Senate committees by the Republican leadership in both houses. Why are the Congressional Republicans opposed to paper validation of e-voting machines?*

2. Why will the Edison Media Research and Mitofsky International not release the raw exit polling data from the Ohio election? What reasons do they give for the alleged "error" in the early Ohio exit polls?

3. Why were exit polls in uncontested states and states with auditable returns extremely accurate, while the exit polls in the "battleground states" were not?

4. Why did almost all the exit poll "errors" throughout the US favor Bush, while the very few exceptions were all within the margin of error?

5. What are the odds of this happening, purely "by chance?" Qualified statisticians (e.g. Dr. Steven Freeman ,Jonathan Simon , and Dr. Ron Baiman) have calculated these odds to be "statistically impossible." Why are these statistical analyses not scrupulously rebutted, but instead are ridiculed or else simply ignored?

6. Without question, many laws were broken (especially in Ohio), specifically the federal "Voting Rights Act." In Nevada and Oregon, Democratic registration forms were trashed, and so noted by competent witnesses. Why are there no indictments?

7. In the 2000 election, Republican staff members from Washington were flown down to Miami, where they disrupted and shut down an official government activity – the recounting of ballots. Why were there no indictments?
8. Do all the above questions add up to "reasonable doubt" that the election of 2004 was fair, and that subsequent elections will be fair? Is this a degree of "reasonable doubt" that might lead a grand jury to indict?

9. If, as the accusers contend, the party in control of the unauditable machines and the secret software can not be voted out of office, can that government in any sense be said to possess "the consent of the governed", and can the US government be said to be a democracy?

10. Can we therefore afford not to investigate these accusations and thus to continue to use voting machinery that is not secure and verifiable? Can we, in short, allow ourselves to "just get over it"?

11. When such questions as these arise, why should the burden of proof be placed on the skeptics? Don't we, as citizens, have the right to expect that the elections are fair, and that our government will establish rigorous and public safeguards to secure that right? (See my " Do We Still Have a Democracy?)

12. Why have the above questions rarely been raised and investigated in the mainstream media?

And finally:

13. *Suppose you wanted to set up a fraudulent voting system that would assure victory for your party and yet con the public into believing the system was fair and accurate. How could you improve upon the e-voting system in place – with its secret software and its unauditable and unverifiable "output," combined with a totally incurious mass media?*

These questions must be asked, repeatedly and relentlessly, until they are either plausibly answered or, more likely, the public finally comes to realize and appreciate that there are no acceptable answers to these questions. For it is becoming ever-more apparent that the authentic though hidden and unspoken answers to these questions must lead to the inescapable conclusion that our national elections are farces and frauds, and that we the people have thus lost the capacity to replace our government through the ballot box. If this is the case, that government, put simply, no longer rules with "the consent of the governed."

We must therefore demand the return of fair and verifiable elections and with that realization, the restoration of government of, by and for the people. And we must devoutly hope that this can be accomplished peacefully. For as John F. Kennedy warned: *"Those who make peaceful revolution impossible, will make violent revolution inevitable."*

****

Bio-Tag: Dr. Ernest Partridge is a consultant, writer and lecturer in the field of Environmental Ethics and Public Policy. He publishes the website, "The Online Gadfly" (www.igc.org/gadfly) and co-edits the progressive website, "The Crisis Papers" (www.crisispapers.org).

Home Page |Headlines |Previous Story |Next Story
http://www.scoop.co.nz/mason/stories/HL0502/S00038.htm

Ernest Partridge
Co-Editor "The Crisis Papers"
February 1, 2005
From: www.crisispapers.org/essays-p/shut-up.htm

Bayer, David

From: David Bayer [bayer2@dcn.org]

Sent: Monday, February 21, 2005 11:27 PM

To: Undisclosed-Recipient:@csus.edu;

Subject: Need for California Voting Analyses: Four Strategic Studies and WHO NOT TO TRUST or ASK

Amigos:

Acting in good faith, I sent the January 12 email below. None of those to whom it was sent have had the courtesy to respond. It has been more than a month. It is not the first time that the political people addressed in the email have NOT responded to my requests for an investigation into the California elections.

I now know why Ms. Alexander did not respond. This was confirmed by friends who attended her Sunday night "show" (February 20) in Sacramento. Fundamentally, she believes that the election of 2004 went along fine with regard to the electronic voting machines (as she was quoted in the Davis Enterprise). Ms. Alexander will have nothing to do with any questioning about the discrepancy between the polls before the election and the exit polls versus the election outcome. **Apparently, anyone who raises these questions or calls for investigations is a "conspiracy theorist" in her eyes, unworthy of any discussion or attention.**

The real conspirators are these very people, politicos and defenders of the 2004 election. By refusing to exam these discrepancies they have cast out the foundation stone of SCIENCE which is based on these very statistical methods. Therefore it is they, not us, who are the complicit criminals since they would have us believe in "faith" rather than science as related to voting processes. In this sense, they have joined the "faith based camp" of busites who prefer to practice THE BIG LIE as opposed to dealing with facts!

At the WASHINGTON, DC, Nov. 20, 2004 press conference in The Governor's House Hotel, representatives of the 'Election Verification Project', a coalition of
technologists, voting rights and legal organizations..."Kim Alexander, of The California Voter Foundation, sang the praises of touchscreen machines, despite the
mayhem she admits their use caused in this year's election" ... Alexander added to the confusion at the press conference when she boasted that " . . . there was no nation-wide meltdown." By Lynn Landes, Online Journal Contributing Writer http://onlinejournal.com/evoting/112004Landes/112004landes.html .

When confronted by me in a private email with the above citation, Ms. Alexander claimed that the CVF has always had a position that electronic voting machines must have paper ballots. However, when I requested that she work with me to insist that Shelley **REQUIRE (not leave optional) paper ballots for the counties like Orange, Riverside and San Bernardino (see the Proposition 66 analysis below)** Ms. Alexander ignored the request.

The bottom line is that Ms. Alexander is just another apologist for electronic voting. If you are interested in democracy and the voting rights of citizens, do not TRUST or depend on information or backup from the CVF. Like many other such organizations which are beholden to corporate contributions, CVF is in business to PROTECT the existing power structure and corrupted system of democracy, a mere carcass stripped of its meat (fair elections and a free press). CVF financial supporters are interlocked with computer companies and others which stand to gain with the widespread use of electronic voting equipment.

Unfortunately, the "politicos" and "yellow" press love to consult Ms. Alexander because she "sings the praises" of electronic voting systems without demanding the following safeguards:

1- a paper ballots for each vote cast, locked in boxes and saved for a recount.

2- obligatory recounts based on sampling the votes in each precinct to make sure that each electronic total in each precinct matches the sample drawn. We are NOT interested in how close the vote is or if there was a landslide for one candidate or issue (e.g. Proposition X). OBLIGATORY RECOUNT MEANS EXACTLY WHAT IT SAYS: a random sample of the paper ballots must be drawn to check its results with the electronic results at each precinct!

3- Polls: Pre-voting polls (three days before the election) and Exit Polls are additional guarantees of voting integrity (read: preventing fraud). In fact, Exit Polls are the most important mechanism for preventing fraud

whether or not electronic voting technologies have been used.

Exit polls should be required to be executed by every Secretary of State. Other entities can do them. But there is NO EXCUSE for these not being done by the States.

4- The entire voting system must be in public hands. There should be NO private enterprise participation in the voting process. The Secretary of State position in each state of the union should be NONPARTISON.

In summary, all those interested in genuine democracy will have to work with progressive organizations and set up their own media and systems of communications. The existing power structure, Democrats and Republicans alike, have become too confortable and corrupt with their power.

david

---- Original Message -----

From: David Bayer
To: Kim-CalVoter
Cc: Lois Wolk ; Senator Machado ; Senator Perata
Sent: Wednesday, January 12, 2005 11:30 AM
Subject: Need for California Voting Analyses: Four Strategic Studies

Kim Alexander
President, California Voter Foundation
kimalex@calvoter.org,
916-441-2494
http://www.calvoter.org
http://www.calvoter.org/news/blog
Dear Kim:

Can you please assign team projects in the California Voter Foundation to analyze the following voting outcomes:

I- the 210,000 less votes for Kerry than Boxer:

I have not finished with the California data but it would seem that the six Touch Screen counties accounted for the 210,000 excess Bush votes relative to the Senatorial candidates: Kerry got 210,000 less votes than Democratic Senator Barbara Boxer. These votes were most likely transferred to Bush who got 954,000 more votes than Republican Senatorial candidate, Bill Jones. We call this "spread analysis". (Bayer email 25 December 2004)

II- Prop 66 analysis:

Where did the winning votes come from which changed the "yes" vote to a "no" vote ....a 22 percent shift in less than a week:

"Like Prop 57 ($ 15 billion bond issue where Arnold "paid off " the banks) in the March primary, Prop 66 (Three Strikes Overhaul) is headed for defeat.

On October 12, the Field Poll showed it winning by 65 to 18 percent.

On October 27, the Field Poll showed it winning by 55 to 33 percent with the trend in the direction of loosing.

We are told by the "controlled" media and press that Arnold S. is against Prop 66. He has T.V. spots against it which are heavily financed by big capital and the prison guard unions (was not he supposed to reform this sector?). We are told by NEWSPEAK people that Arnold is very popular and that what he says, goes.

The Field Poll and Newspeak are preparing us for the touch screen computer fixes in the heaviest population areas of California: there Prop 66 will be voted down many times the multiple of the state average as was the case for Proposition 57 which swung from being defeated a week before the election to winning, a shift of nearly 40 percent." (Bayer email 30 October 2004).

19 February 2005 Up-date: Bayer analysis finds the following:

The three largest DRE counties (Orange, Riverside and San Bernardino) produced more than two times the number of votes against Proposition 66 by which Proposition 66 lost : 1,296,339 versus 634,000. The average "vote against" in each of these counties was 10 percent points above the state average (62 % versus 53 %). Since there is NO PAPER TRAIL, there is no way for election officials to demonstrate that this outcome was not manipulated. The public is asked to have "faith" in this highly unpredictable outcome?

III- **Prop 57:**

In this case there was a 40 percent shift over two weeks. How did it win? Where did the winning votes come from? Begin hand sampling the votes in the counties to determine if the samples correspond to the electronic precinct totals.

Bayer analysis is pasted as the last table at the end of this email.

IV- **Arnold Schwarzenegger election of October 2003:**

How did he win?

Follow-up on the Bayer analysis and the "Independent" analysis (both documents are pasted as the first two at the end of this email).

You may be able to request monies for these studies from the state legislature and you may be able to get the UC Berkeley team of Sociolgists which did the Analysis of Variance Study on the 15 Touch Screen counties in Florida to participate and/or accept a contract.

I have requested that members of the state legislatures (Wolk, Machado and Perata) distribute Bayer's "California Governor Race Oct-2003"document attached (they received it in two previous emails) to all other members of the state legislature and call for an investigation / research analysis. This document has previously been shared with California Secretary of State, Kevin Shelley, and his staff. THEY APPARENTLY TOOK NO FURTHER ACTION except to email me, trying to explain away the results by talking about the high Republican registration from the heavy Schwarzenegger counties. This explanation is pure " you know what" since none of these counties has five times or three times Republican over Democratic registration (which ever way you want to read my table). **NO SERIOUS SCIENTIFIC FOLLOW-UP ANALYSIS AND /OR CRITIQUE HAS BEEN DONE RELATIVE TO THE GOVERNOR'S ELECTION.**

Kim:

Unless these analyses are done and unless we begin to get at the bottom of electoral fraud, we are NOT going to protect the citizen voter. The four items above are California events. The votes DO NOT ADD UP just like they DO NOT add up for the rest of the 2004 presidential election.

Your Foundation has a real opportunity to make a major contribution. This is NOT political ideology or rhetoric. Please have your people begin to look at the numbers.

I may be able to assist in some of this and meet with you.

Sincerely,

david

David Bayer

6/13/2005

1912 Haussler Drive
Davis, CA 95616

Tel: 530-759-2004
email: bayer2@dcn.org

CALIFORNIA GOVERNOR RACE

MACHINE ANALYSIS FOR RECALL ELECTION OCTOBER 2003

EVIDENCE THAT THE ELECTION WAS FIXED

STATE RESULTS:

Cruz Bustamante (CB)= 32 %
Arnold Schwarzenegger (AS)= 49 %
Ratio AS / CB = 1.5

A- Mark Sense Ballot Card using Diebold- Accuvote OS machines:

County	CB %	AS %	Ratio AS/CB
1-Fresno	28	52	1.9
2-Humboldt	36	42	1.2
3-Kern	19	62	3.3
4-Lassen	15	61	4
5-Marin	48	32	.7
6-Modoc	14	61	4.4
7-Placer	17	63	3.7
8-San Joaquin	27	49	1.8
9-San Luis Obispo	26	50	1.9
10- Santa Barbara	31	47	1.5
11-Siskiyou	20	59	3
12-Trinity	22	53	2.4
13-Tulare	23	56	2.4

B- Touch Screen machines:

1- Diebold Accu-Vote :

14-Alameda	**54**	**26**	**.5**
15-Plumas	**20**	**55**	**2.8**

2- Sequoia Pacific AVC Edge:

16-Riverside	**22**	**61**	**2.8**
17-Shasta	**17**	**58**	**3.4**

TOTAL **41.7**

TOTAL MUST BE DIVIDED BY 17 TO GET AVERAGE = 2.5

ANALYSIS:
1- Schwarzenegger got 2.5 times as many votes as Bustamante from the DRE and Diebold machines on the average.

2- Schwarzenegger got 5/10 of as many votes as Bustamante from all the other non-DRE and non-Diebold machines used. That is, on the average, Bustamante beat Schwarzenegger on all the other machines.

$$\frac{.5\ S/B\ +\ 2.5\ S/B}{2} = 1.5\ S/B$$

where 1.5 is the State ratio of Schwarzenegger's votes to Bustamante's.

3- The DRE and Diebold machines produced the victory for Schwarzenegger, producing five times (5) as many votes for him relative to what the non-DREs produced for Bustamonte: 2.5 divided by .5 = 5 .

DRE= Direct Recording Electronic (paperless) voting machines. All the percentages come from the California Secretary of State Data Base.

Wednesday, October 08, 2003
IRREGULARITIES IN CALIFORNIA RACE!!

Long-shot candidates do startlingly well in Tulare County

DIEBOLD MACHINES YIELD FISHY RESULTS!!

My friend in South Carolina writes:

I ran a number crunch of CA counties that use Diebold machines to cast/count votes and found some weird figures that show a skim of votes from top candidates to people who were unlikely to affect the outcome. I did my hand calculator work on the California election results (from the secretary of state's site) when 96% of precincts had reported. The website showed:

Counties using Diebold Touchscreens:
Alemeda, Plumas

Counties using Diebold Optiscan:
Fresno, Humboldt, Kern, Lassen, Marin, Placer, San Joaquin, San Luis Obispo, Santa Barbara, Trinity, Tulare.

There were a total of 1,403,375 votes cast in these counties combined. The CA total was 7,842,630 at this stage of the count. Thus 17.89% of all the state votes were cast/counted on Diebold equipment.

I had earlier noticed some lower order candidates (ones who couldn't affect the result) were getting unusually large numbers of votes in Tulare county. I decided to test to see if the these and other 'fringe' candidates might be used to receive skimmed votes in other Diebold counties.

Method:
I added all the votes cast/counted on Diebold equipment for each candidate and expressed it as a percentage of their total votes cast state wide. The following table lists: Candidate name, votes counted for them in Diebold counties, CA state total votes counted for that candidate and what percentage of that candidate's total votes were counted in Diebold counties.

It looks like, as one might expect, at the top of the list as if there is a slight variance from an even state wide distribution. However many 'lower ticket' candidates have vote totals that ONLY correlate with the use of Diebold equipment! I have included some names chosen at random from the result list that show that not all lower order candidates were used to receive skimmed votes. Note that Diebold's counties are spread geographically over the whole of California.

I have checked background on the skewed result candidates and they are not residents of the counties where they got very high percentage results. In one case, Palmieri, the candidate was surprised to hear about Tulare county (I emailed him) and had not been there nor had family or friends there. In fact, his platform was "Don't vote for me." He described this vote pattern as "strange."

State total 7,842,630.
Cast in Diebold counties 1,403,375

17.89% of the total votes cast.

Schwarzenegger 581,145 3,552,787 16.36%

Bustamante 447,008 2,379,740 18.78%

McLintock 186,923 979,234 19.08%

Camejo 39,199 207,270 18.9%

Huffington 7,498 42,131 17.79%

Ueberoth 3365 21378 15.74%

Flynt 2384 15010 15.88%

Coleman 1869 12443 15.02%

Simon 1351 7648 17.66%

Palmieri 2542 3717 68.3%

Louie 598 3198 18.7%

Kunzman 1957 2133 91.75%

Roscoe 325 1941 16.7%

Sprague 1026 1576 65.10%

Macaluso 592 1504 39.36%

Price 477 1011 47.18%

Quinn 220 433 50.8%

Martorana 165 420 39.28%

Gosse 60 419 14.3%

Conclusion
Based on the very unlikely distribution of votes for some candidates (a meteor hit my car twice this week sort of odds) a hand count of the affected counties to compare with the machine reported count should be done. This would show that the machines had been tampered with to alter the results. As we already know, it is not possible to audit touchscreen machines because Diebold refuse to allow printing of a ballot to be placed in a box as a back up for use in just such an apparent tampering with votes.

For those who are unsure of figures:

California is huge and has a population similar to many European nations. Lower order candidates had little or no ability to spread any sort of message to parts of the state beyond their own home and/or where they have previously lived. One would expect some of the 'fringe' candidates to do well in their home county and then to have a very even distribution across the rest of the state. That is not the case. In Diebold counties (those who use machines made by Diebold, a corporation that supports George Bush) the

results are skewed towards low scoring candidates by unbelievably large amounts.

The probability of scoring twice the expected average county % could charitably be construed as the upper limit of the possible. Some candidates exceed that figure in Diebold counties by a four or five fold margin. If you have done statistics, you know that is so far beyond what might be expected that you would reject it as defective data. If it happened to one candidate in this election, I would be surprised but might accept it. There are a large number of candidates who have this same systematic pattern of receiving skimmed votes.

The California recall shows Diebold trying to affect the election outcome by moving votes from high ranked candidates to low ranked candidates.

By doing this, Diebold keep the total number of votes cast constant but rob some candidate of their votes. Before anyone makes this a partisan issue - it could be a Republican victim next time.

 # posted by mark @ 11:08 PM

CALIFORNIA March 2004 Primary

MACHINE ANALYSIS FOR PROPOSITION 57

STATE RESULTS:

YES = 63.4 % WITH 4,056,313 VOTES
NO = 36.6 % WITH 2,348,910 VOTES
Ratio YES / NO = 1.7

A- Mark Sense Ballot Card using Diebold- Accuvote OS machines:

County	POP -YES	YES %	NO %	Ratio YES/NO
1-Fresno	81,000	59	41	1.4
2-Humboldt		48	52	.9
3-Kern	73,000	64	36	1.7
4-Lassen		57	43	1.3
5-Marin	51,000	62	38	1.6

6-Mendocino		**57**	**43**	**1.3**
7-Modoc		**49**	**50**	**.9**
8-Placer	**62,000**	**67**	**33**	**2.0**
9-San Diego	**428,000**	**71**	**29**	**2.4**
10-San Joaquin	**63,000**	**63**	**37**	**1.7**
11-San Luis Obispo	**46,000**	**59**	**40**	**1.5**
12- Santa Barbara	**57,000**	**58**	**42**	**1.4**
13-Siskiyou		**53**	**47**	**1.1**
14-Solano	**47,000**	**61**	**39**	**1.6**
15-Trinity		**50**	**50**	**1.0**
16-Tulare	**37,000**	**65**	**35**	**1.9**

B- Touch Screen machines:

1- Diebold Accu-Vote :

17-Alameda		**55**	**45**	**1.2**
18-Plumas	**4,000**	**61**	**39**	**1.5**

2- Hart eSlate

19- Orange	**374,000**	**67**	**33**	**2.0**

3- ES&S iVotronic

20- Merced	**19,000**	**63**	**37**	**1.7**

4- Sequoia Pacific AVC Edge:

21- Napa	**21,000**	**59**	**41**	**1.5**
22-Riverside	**187,000**	**71**	**29**	**2.4**
23-San Bernadino	**171,000**	**70**	**30**	**2.3**

24-Shasta		**50**	**50**	**1.0**
25-Santa Clara	**202,000**	**64**	**36**	**1.8**
26-Tehema		**50**	**50**	**1.0**
5- Inka Vote				
27- Los Angeles	**813,000**	**59**	**34**	**1.7**

Total of 18 Counties with ratio of 1.4 or above = 2,736,000 votes.

NEARLY 3 million OF THE VOTES CAST TO PASS PROPOSITION 57 WERE CAST IN 18 OF 58 COUNTIES.

Eleven OF THESE COUNTIES HAD RATIOS OF YES/NO AT OR ABOVE THE STATE AVERAGE OF 1.7. Nine OF THE 11 WERE THE MOST POPULOUS COUNTIES AND HAD RATIOS ABOVE 1.7.

Conclusion: The DERs in the 18 counties identified above produced a disproportionate number of votes in favor of Proposition 57. If DERs had not been used in these counties, it is more than likely that Proposition 57 WOULD NOT HAVE PASSED!

VOTER FRAUD IN 2004: THE CASE OF PROPOSITION 66

19 FEBRUARY 2005

DAVID BAYER

Analysis of Proposition 66, Limitations on Three Strikes Law

One week before the November 2,2004 election, the polls showed Proposition 66 passing by 66 percent to 34 percent:

State Totals:

For---5,604,060.....47.3 percent

Against---6,238,060.....52.7 percent.....lost by 634,000 votes.

In three Touch Screen Counties, the vote **against** was as follows:

Orange----------641,073.....62 percent

Riverside---------331,932.....61 percent

San Bernardino--322,981.....64 percent

Total 1,296,339 62 percent average.....10 percent above state average

These three counties produced more than two times the number of votes against Proposition 66 by which Proposition 66 lost : 1,296,339 versus 634,000. The "vote against" in each of these three counties was 10 percent above the state average.

THERE IS NO WAY FOR THESE THREE COUNTIES TO PROVE THAT PROPOSITION 66 LOST BY THE AMOUNTS RECORDED IN THESE COUNTIES.

THERE IS EVERY REASON IN THE WORLD—ESPECIALLY THE POLLS— TO DOUBT THESE RESULTS. THEY SHOULD BE CHALLENGED.

David Bayer
1912 Haussler Drive
Davis, CA 95616

Tel: 530-759-2004
email: bayer2@dcn.org

CALIFORNIA GOVERNOR RACE

MACHINE ANALYSIS FOR RECALL ELECTION OCTOBER 2003

EVIDENCE THAT THE ELECTION WAS FIXED

STATE RESULTS:

Cruz Bustamante (CB)= 32 %
Arnold Schwarzenegger (AS)= 49 %
Ratio AS / CB = 1.5

A- Mark Sense Ballot Card using Diebold- Accuvote OS machines:

County	CB %	AS %	Ratio AS/CB
1-Fresno	28	52	1.9
2-Humboldt	36	42	1.2
3-Kern	19	62	3.3
4-Lassen	15	61	4
5-Marin	48	32	.7
6-Modoc	14	61	4.4
7-Placer	17	63	3.7
8-San Joaquin	27	49	1.8
9-San Luis Obispo	26	50	1.9
10- Santa Barbara	31	47	1.5
11-Siskiyou	20	59	3
12-Trinity	22	53	2.4

13-Tulare	**23**	**56**	**2.4**

B- Touch Screen machines:

1- Diebold Accu-Vote :

14-Alameda	**54**	**26**	**.5**
15-Plumas	**20**	**55**	**2.8**

2- Sequoia Pacific AVC Edge:

16-Riverside	**22**	**61**	**2.8**
17-Shasta	**17**	**58**	**3.4**

TOTAL **41.7**

TOTAL MUST BE DIVIDED BY 17 TO GET AVERAGE = 2.5

ANALYSIS:
1- Schwarzenegger got 2.5 times as many votes as Bustamante from the DRE and Diebold machines on the average.

2- Schwarzenegger got 5/10 of as many votes as Bustamante from all the other non-DRE and non-Diebold machines used. That is, on the average, Bustamante beat Schwarzenegger on all the other machines.

$$\frac{.5\ \text{S/B} + 2.5\ \text{S/B}}{2} = 1.5\ \text{S/B}$$

where 1.5 is the State ratio of Schwarzenegger's votes to Bustamante's.

3- The DRE and Diebold machines produced the victory for Schwarzenegger, producing five times (5) as many votes for him relative to what the non-DREs produced for Bustamonte: 2.5 divided by .5 = 5 .

DRE= Direct Recording Electronic (paperless) voting machines. All the percentages come from the California Secretary of State Data Base.

NO DIEBOLD ELECTRONIC VOTING MACHINES IN CALIFORNIA!

We the undersigned oppose the use of Diebold Electronic Voting machines in California. There is strong reason to believe that the Diebold Company may have "delivered" Ohio and other states to George Bush (to use the words of Diebold's CEO at a Bush fundraiser.)

Statisticians from around the country have calculated that the probability of random error in the exit polls from precincts that favored Kerry but ending up "voting" for Bush are 1 million to 1. The Bush administration, in typical hypocritical fashion, used exit polls as a basis for calling the Ukrainian Election fraudulent, whereas the deemed exit polls "wrong" in the 2004 presidential election.

So far, Diebold has not allowed the software of their machines to be inspected by non-partisan experts to see if there were glitches in the programming or if the machines were deliberately programmed to favor Bush. They hide behind patent protection laws. Until there is a complete, impartial investigation of the Diebold machines and the company's impact on the results of the 2004 election, no further contracts should be awarded to Diebold. Indeed, if the suspicions of a large number of American voters are proven correct, jail sentences for those responsible for the alleged stealing of the 2004 election would be more appropriate.

	NAME: (1) Print and (2) Sign	ADDRESS	CITY	ZIP CODE	PHONE
1	Lana Kitchel Lana Kitchel	P.O. Box 194, 25255 3rd Ave.	Los Molinos	96055	(530) 384-1966
2	Georgianna Summers Georgianna Summers	1012 Francesca Dr.	Chico	95973	(530)899-9464
3	Matba Hazzard Matba Hazzard	1937 Flamingo Rd.	Chico	95926	(530)345-1895
4	CAROL EBERLING Carol Eberling	1555 Vallombrosa Apt #63	Chico	95926	" 892 9026
5	Gene Anna McMillan Gene Anna McMillan	2040 Vallombrosa Ave	Chico	95926	(530) 345-7003
6	Oden J. McMillan Oden James McMillan	"	"	"	"
7	Charles L. Neumann Charles L. Neumann	1810 Paige Ln.	Paradise	9589	(530) 877-3985
8	Carole A. Neumann Carole A. Neumann	1810 Paige Lane	Paradise	95969	530 877 3965
9	JOHN KITCHEL John Kitchel	25255 3rd Ave	Los Molinos	96055	530-384-1966
10	Dawn Boatto Dawn Boatto	2846 Jolyn Wy Apt B	Chico	95973	530-345-1242
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

NO DIEBOLD ELECTRONIC VOTING MACHINES IN CALIFORNIA!

We the undersigned oppose the use of Diebold Electronic Voting machines in California. There is strong reason to believe that the Diebold Company may have "delivered" Ohio and other states to George Bush (to use the words of Diebold's CEO at a Bush fundraiser.)

Statisticians from around the country have calculated that the probability of random error in the exit polls from precincts that favored Kerry but ending up "voting" for Bush are 1 million to 1. The Bush administration, in typical hypocritical fashion, used exit polls as a basis for calling the Ukrainian Election fraudulent, whereas the deemed exit polls "wrong" in the 2004 presidential election.

So far, Diebold has not allowed the software of their machines to be inspected by non-partisan experts to see if there were glitches in the programming or if the machines were deliberately programmed to favor Bush. They hide behind patent protection laws. Until there is a complete, impartial investigation of the Diebold machines and the company's impact on the results of the 2004 election, no further contracts should be awarded to Diebold. Indeed, if the suspicions of a large number of American voters are proven correct, jail sentences for those responsible for the alleged stealing of the 2004 election would be more appropriate.

	NAME: (1) Print and (2) Sign	ADDRESS	CITY	ZIP CODE	PHONE
1	Charles Rose Charles Rose	1737 Flamingo Rd	Chico	95926	332-9474
2	ERIC DEKKER E-Jr	626 CAPP ST. #201	SF	94110	
3	ALAN DEKKER A L D K	927 S. VAN NESS	SF	94110	
4	David L. Moss David L. Moss	880 E 6th St.	Chico, Ca.	95928	898-0806
5	Lucille F. Rocks Lucille Rocks	1228 Glenn Haven Dr	Chico CA	95926	
6	JANIS W. CHISHOLM Janis W. Chisholm	1179 Honey Run Road	Chico CA	95928	~~895-0213~~
7	Leslie Johnson L Johnson	PO Box 7655	Chico CA	95927	530 342-6112
8	June E. Rothe-Barneson June Rothe-Barneson	738 Downing Ave	Chico CA	95926	(530) 342-3994
9	Patsy L. Barklow - Patsy L. Barklow	1726 Flamingo Rd	Chico CA	95926	
10	Ellis E. Barklow ELISE BARKLOW	1726 Flamingo Rd	CHICO CA	95926	
11	Marba Hazzard Marba Hazzard	1737 Flamingo Rd.	Chico, CA	95926	(530) 345-1895
12					
13					
14					
15					
16					
17					
18					
19					
20					

NO DIEBOLD ELECTRONIC VOTING MACHINES IN CALIFORNIA!

We the undersigned oppose the use of Diebold Electronic Voting machines in California. There is strong reason to believe that the Diebold Company may have "delivered" Ohio and other states to George Bush (to use the words of Diebold's CEO at a Bush fundraiser.)

Statisticians from around the country have calculated that the probability of random error in the exit polls from precincts that favored Kerry but ending up "voting" for Bush are 1 million to 1. The Bush administration, in typical hypocritical fashion, used exit polls as a basis for calling the Ukrainian Election fraudulent, whereas the deemed exit polls "wrong" in the 2004 presidential election.

So far, Diebold has not allowed the software of their machines to be inspected by non-partisan experts to see if there were glitches in the programming or if the machines were deliberately programmed to favor Bush. They hide behind patent protection laws. Until there is a complete, impartial investigation of the Diebold machines and the company's impact on the results of the 2004 election, no further contracts should be awarded to Diebold. Indeed, if the suspicions of a large number of American voters are proven correct, jail sentences for those responsible for the alleged stealing of the 2004 election would be more appropriate.

	NAME: (1) Print and (2) Sign	ADDRESS	CITY	ZIP CODE	PHONE
1	Berda R. Lydon Berda R. Lydon	2948 San Verbena Loop	Chico	95973	530-343-9277
2	WENDY WOODS Wendy Woods	40 Dominion Dr.	Chico	95973	530 899-8607
3	Joanne Gerson Joanne Gerson	977 Palmetto	Chico	95926	530-893-2154
4	Lynn Ott	5832 Ingalls Rd.	Paradise	95969	530-877-1671
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

THE CASE FOR FRAUD IN THE 2004 ELECTION

David Benavides, 18 May 2005

The single most important issue of our times is the question of vote fraud. This essay demonstrates beyond any reasonable doubt that something went terribly wrong in the November 2, 2004 Presidential election. Whether you accept or reject the fraud thesis, you are compelled to review the evidence if you take our democracy seriously. Given that the mainstream media refuses to discuss the fraud possibility, not only is the "right of the people to choose their representatives" under attack but the second pillar of democracy, "freedom of the press" appears to be under siege.

PART I

WE NO LONGER LIVE IN A DEMOCRACY

The United States of America lost its claim to being a democracy with the 2000 election of George W. Bush.

The official story put out by the mass media points to a close election in Florida where Bush beat Gore by a couple of hundred votes. The Florida Supreme Court ordered a recount, but the U.S. Supreme Court over-ruled Florida, handing Bush a victory. Two dissenting U.S. Supreme Court Justices, John Paul Stevens and Ruth Bader Ginsburg, stated that the highest court in the land had "no legal basis" for intervening in the election since election processes are managed by each state according to the United States Constitution. Even if we accept the "the close vote story", the election of GWB was illegal.

The real story is that Governor Jeb Bush and Florida Secretary of State Katherine Harris hired ChoicePoint, a private company, to remove the names of 100,000 Florida voters from the rolls, predominately in minority areas in Miami-Dade county, who would have voted sixty percent for Gore. In short, Gore would have beaten Bush easily by 20,000 votes.

This act of treason by Republicans in fixing the 2000 election was surpassed by the complicity of the Democratic Party: not one Senator joined the Black Congressional caucus in protesting Florida's electoral votes during the January 2001 certification process. This was the real shame of the USA: the Party of the people sold out and refused to fight for democracy!

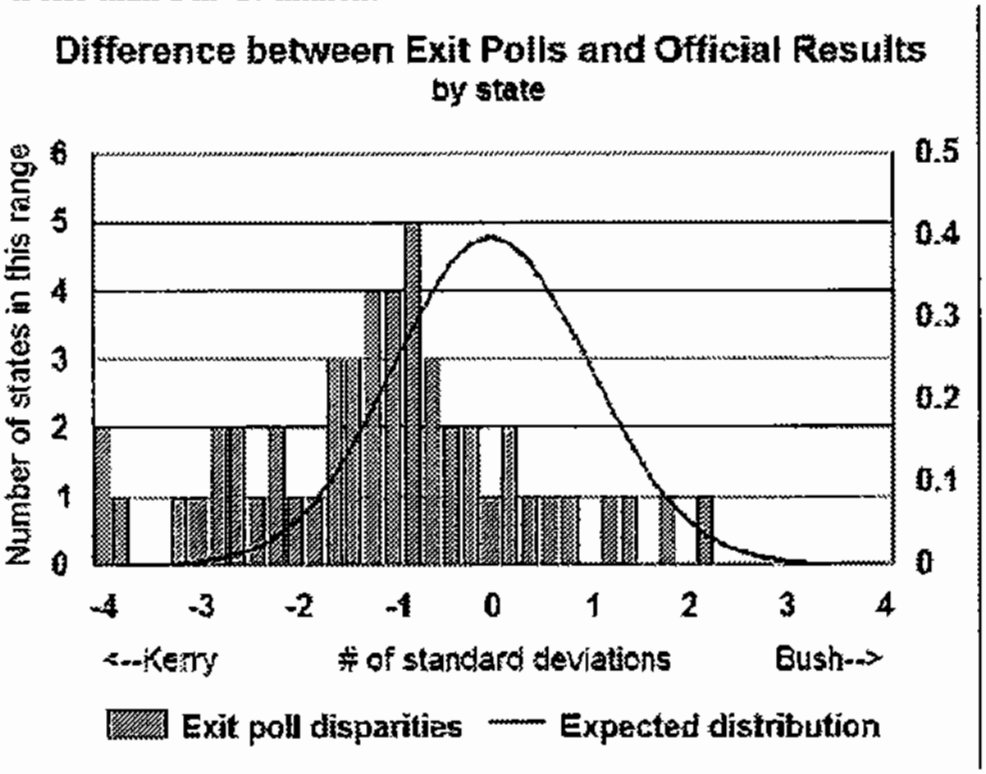
Democratic weakness emboldened the Republicans who set out to fix the 2004 election, projecting their domination for another four years both in the House and Senate. The trick was to use the Florida vote-counting fiasco as an excuse to move to electronic voting throughout the USA. Republicans achieved their goal when sixty five percent of the 160 million votes on November 2, 2004 were counted on electronic machines throughout the USA with half of these being "paperless" direct

electronic recording, voting machines (DREs) without any possibility of doing a recount. To underscore their intentions, Jeb Bush stated before the election: "There will be no recount in Florida".

The proof for the fixing of the 2004 election is ample and extensive. It can be found throughout the internet websites. One of the best is Gary Beckwith's http://election.solarbus.org/ . There you will find several major scientific studies by leading scholars which demonstrate beyond any reasonable doubt that Bush did NOT win the electoral vote (e.g. he did NOT win Ohio and Florida) or the popular vote. The Executive Summary of the definitive report, "Response to the Report Evaluation of Edison/Mitofsky Election System 2004", by the US Count Votes' National Election Data Archive Project is located at http://electionarchive.org/ucvAnalysis/US/Exit_Polls_summary.pdf . **It can be paraphrased as follows:**

1- **The weighted national exit poll, conducted by Edison/Mitofsky, predicted Kerry to win the popular vote by 3 % but the official vote count had Bush winning by 2.5 %. This discrepancy of 5.5 % is the largest in the poll's history, representing 5 million less votes for Kerry and 3 million excess votes for Bush: a total of 8 million stolen votes.**

2- **Seven of fifty states (DE;MN;NH;NY;VT;SC;PA) have t values less than – 2.7, meaning that each of their discrepancies had less than 1 % probability of occurring by chance. The probability that 7 of 50 states should be so skewed is less than 1 in 10 million:**



This means that random error must be ruled out as an explanation for the difference between election results and exit polls. Only two other possibilities remain: bias in the exit polling process or a systematic stealing of votes from Kerry and their transfer to Bush. For the bar graphs to be this far away from zero in the normal bell curve means that something was way off -either the exit polls or the official vote count. Edison/Mitofsky International agreed that something was definitely wrong and stated it was their own nationwide exit polls.

3- **Edison/Mitofsky concoct a story that Bush voters were "shy/reluctant to answer the pollsters" and therefore, there was a systematic bias in the polling process since, within the 70,000 nationwide respondents, Kerry voters were over-sampled. The US Count Votes study demonstrates that Edison/Mitosky's own polling data does not and cannot support this fabrication. In fact, the Edison/Mitosky data supports the opposite conclusion: (1) response to exit polls were slightly higher in Republican precincts compared to Democratic precincts and (2) exit poll discrepancies are highest where Bush voters predominated.**

4- **The Edison/Mitosky exit poll underscores a systematic bias in the official vote count. The corruption of the vote counting process overwhelmingly favored Bush: in 40 of the 50 states the exit polls showed Kerry winning but the vote count was fixed by the machines (not the voters) to favor Bush.**

5- **Given the above scientific evidence and the fact that Edison/Mitosky has refused to release all their raw exit poll data, the 2004 Presidential election merits a full investigation and exhaustive recount in the key swing states such as Florida and Ohio.**

The full US Count Votes report can be found at:
http://electionarchive.org/ucvAnalysis/US/Exit_Polls_2004_Edison-Mitofsky.pdf

The May 17, 2005 up-date can be found at:
http://uscountvotes.org/ucvAnalysis/US/exit-polls/USCV_exit_poll_simulations.pdf

An easy to read companion article, "A Corrupted Election: Despite what you may have heard, the exit polls were right" (Steve Freeman and Josh Mitteldorf, In These Times, February 15, 2005) can be found at:
http://www.inthesetimes.com/site/main/print/1970/

The results in New York State, which did not use electronic voting machines, demonstrate that Kerry beat Bush by a landside: 58 percent to 40 percent. People exaggerate by saying that New York is radically different from the other 49 states. The facts are that New York has a Republican Governor and rural New York is strongly Republican. If you want to compensate for New York's differences: cut the

18 percentage point difference in half or again into quarters—the result is still a landslide in favor of Kerry.

The vast majority of the voters had no confidence in the election process. Just prior to November's election, a CBS/NYT poll indicated that only 35% of registered voters had full confidence that their votes would be counted properly. That leaves around 100 million people who had only partial, little, or no confidence in America's election process.

Those who deny that the 2000 and 2004 elections were fixed are fooling themselves. The sad truth is that the people in the USA have come to accept and participate in what is "a culture of lies". The mass media promotes the "culture of lies" with false advertising, exaggerated "reality" shows, selling the Iraq War and covering its human horror up by hiding the massive destruction of civilian populations. We now live in George Orwell's 1984 where Big Brother (the Government and Corporate Media) tell the Big Lie. The story about the 2004 election fits this description.

PART II

HOW THE CORPORATE MEDIA SOLD US THE BUSH VICTORY

The mass media went far beyond brainwashing during the 2004 election. ABC, AP (Associated Press), CBS, CNN, Fox, and NBC created the National Election Pool (NEP) to provide tabulated vote counts and exit poll surveys. These organizations appointed Edison Media Research and Mitofsky International as the sole provider of exit polls. The AP collected the vote tallies.

The early CNN/Mitofsky exit polls indicated a Kerry victory in Florida, Ohio, and enough additional states to give Kerry a winning 300+ Electoral College total. The popular vote was projected to be a Kerry win with an exact reversal of Bush's "official" margin: 51%-48%. These projections of a Kerry win were duplicated by the final Zogby poll. Zogby International is a key polling organization.

On election night Kerry was ahead but by early morning Bush was ahead, representing a dramatic shift in the data base. The Exit Polls were contaminated by the Associated Press vote tallies which were fed to the networks. The AP purposely and knowingly mixed the election results from the manipulated electronic machines with the exit poll data (remember exit polls are NOT election results!) in the early hours of November 3, to "force" the exit polls to match the fraudulent election results. Of course, by "contaminating" the exit polls in this manner, they were NO LONGER exit polls but fraudulent results.

Both the New York Times and the MIT/Caltech election analysis team lied to the public by reporting that the earlier exit polls showing Kerry as the winner represented "too small a sample" and an "over-sampling" of Democrats to explain the change in the "exit polls" between 1 to 1:41 AM on November 3. They

have not apologized for this manipulation of public opinion based on unverified voting data and their bias against the possibility of election fraud.

This is the fundamental reason why the corporate media and press have imposed a news BLACKOUT on reporting election fraud: these companies have knowingly participated in the fraud process through the manipulation of election data. All the major media pronounced Bush the "winner". All have a vested interest in maintaining the myth of Bush's re-election! All used the same corrupted vote count data base.

The fundamental questions which the mass media refuses to answer, proving its complicity in fixing the 2004 election, are these:
1- Why was the raw Election Results data mixed with the Exit Poll data in the early hours of November 3? What purpose did this serve? How can it be justified?

2- Why was no step taken or question raised to audit the vote counting procedures and systems in order to find out why there was a discrepancy between the Exit Polls and the Election Results? What justified the assumption that the Exit Polls were wrong and the Election Results right?

3- Given these major discrepancies between Exit Polls and Results, as well as thousands of reports around the nation about voting anomalies, especially in Ohio, why was there a rush to declare Bush the winner without any further analysis?

4- Why has the Media (broadcast and written) been virtually silent on the events above; the Conyers Report http://truthout.org/Conyersreport.pdf.; **the fact that 31 members of the House of Representatives and Senator Barbara Boxer refused to certify Ohio's 20 electoral votes on January 6,2005; the manipulated recount in Ohio; and the major statistical reports which indicate that Kerry won?**

To determine who won the 2004 election all the votes in Ohio and Florida must be hand recounted. Of the 67 Florida counties, 52 used Optical Scan machines which have paper ballots which can be recounted. But 15 counties in the southern part of Florida used DREs, so there cannot be a recount. However, thousands of votes in these counties, including absentee votes were lost and not counted. Given these facts, ***a special election in the 15 Florida DRE counties is justified and should be conducted on Optical Scan voting machines which produce paper trails that could be sampled after the vote to check the electronic outcome. THESE ARE THE MOST POPULOUS COUNTIES IN THE STATE OF FLORIDA.*** **Of the 88 counties in Ohio, only three (which were among the 10 most populous counties) used DREs. Therefore it is possible to recount the vast majority of Ohio's votes plus the 8,000 provisional ballots and the 93,000 "spoiled ballots" which had "no vote for president". If this is to be a real democracy, the votes must be recounted in Florida and Ohio!**

PART III

WHAT IS TO BE DONE?

INVADE WASHINGTON, D.C. AND SET UP DEMOCRACY CITY

People need to take action. Otherwise they will die from depression and repression. By now it must be apparent what Bush represents:

1- **The elimination of Social Security.**
2- **The impoverishment of the middle classes.**
3- **The privatization of the public school system.**
4- **The transfer of wealth to the rich and super-rich.**
5- **Imperial wars to hold or capture oil reserves and markets.**
6- **The termination of labor unions and workers' pensions.**
7- **The destruction of any opposition through the use of "national security" mechanisms and laws to suppress dissent.**

Bush represents a Plutocratic, Corporatist State, which benefits the rich and cloaks itself in religious morality when, in fact, it is one of the most immoral governments which the USA has ever had. People in every Federal bureaucracy are forced to lie and participate in the manipulation of information. The campaign to privatize Social Security is but one example. Before that, there was false Medicare costs and the false reports about global warming put out by the EPA. The war on Iraq was based on lies.

Since oil reserves have "peaked", the USA, which is totally dependent on this source of energy, is now in the first stage of a major crisis. This crisis will be transformed into a "national security" issue. These Plutocrats plan to fix future elections. More DREs will be used in more states. A prime example of this was the removal of California Secretary of State, Kevin Shelley, the only secretary of state in the nation to stand up against the Diebold DREs. If there is any chance that the Plutocrats might loose the next presidential election, it may be postponed with a declaration of a "National Emergency" based on a real or fabricated terrorist attack. The Plutocrats need another ten years to fully remake U.S. society and hold down revolts from the masses. Keep in mind that key Bush operatives (John Negroponte; Elliot Abrams; Richard Armitage; Otto Reich; Colin Powell; plus hundreds of lower echelon operatives loyal to them and past CIA Director George Bush) led the Iran-Contra, extra-official government operation, *THE ENTERPRIZE*, against the will of Congress (e.g. the Boland Amendment). See
http://www.webcom.com/pinknoiz/covert/icsummary.html
http://www.counterpunch.com/mcgovern04272005.html
They lied to Congress and WE THE PEOPLE. They set up their own government. They defrauded the Constitution of the United States. How can anyone doubt that they stole two elections and will not attempt to impose their will no matter who dares to get in their way?

Stealing elections is one more manifestation of the character of the people who now rule the United States. In this sense, the argument for election fraud goes beyond mere statistics and points to the type of people who are willing to engage in this activity and approve its execution.

If the people wait to ride out Bush over the next four years, it will be too late. Our nation as we know it will have been destroyed. Now is the time to take action.

We must occupy Washington, D.C., as soon as possible and create a TENT CITY FOR DEMOCRACY. All the progressive organizations must coordinate and bring millions of people into D.C. to occupy it on a rotational basis. The major goal of this occupation will be to "de-legitimize" the Bush government so that it cannot implement its political program.

The call for mobilizing people to D.C. will be: COUNT THE VOTES IN OHIO AND FLORIDA. The major activities in the TENT CITY FOR DEMOCRACY will be "teach-ins" where experts will explain how the 2004 election was fixed. While we can expect that the U.S. mass media will not televise the "revolution", other, alternative media will, including the foreign press. This will further erode the credibility of the U.S. mass media, forcing it to cover the OCCUPATION.

It is quite possible that a "critical mass" of the population will demand a full recount of the vote in Ohio and Florida, including a new election in Florida's 15 DRE counties, but this time with Optical Scan machines. If this happens, Bush will be legitimately removed from government.

Another major goal in the TENT CITY FOR DEMOCRACY is to set up a CITIZENS COMMITTEE to write the new VOTING REFORM LAW.

This new Voting Reform Law should contain the following elements as recommended by US Count Votes http://uscountvotes.org/ucvAnalysis/US/exit-polls/USCV_exit_poll_simulations.pdf (pages 11-12):

"...
- **full funding of the National Election Data Archive precinct level database.**
- **election equipment that permits access by non-specialist citizen election judges to recount voter verified paper ballots.**
- **routine 3%, randomly selected, independent audits of all elections.**
- **transparent and publicly accessible exit polling.**
- **election administration by non-partisan public civil servants.**
- **non-proprietary open-source coding for all computerized election equipment.**
- **no wired or wireless network connections to any vote casting or counting equipment.**

Vote counts in America need to be routinely and independently audited. It is not enough to require voter verified paper records of ballots. These paper records must be easily and "independently"auditable by persons other than the voting machine vendor, preferably without having to hire computer technicians, paper roll advancers, bar code readers, and laptops, as is true with many voting systems on the market today.

In particular, 3% of randomly selected precincts can be recounted, using the paper record, immediately when polls close, in the precinct, before removing ballots from the precinct. If discrepancies are found, a county-wide recount can be automatically triggered. Additional funding may need to be allocated to state and county election offices to routinely perform independent audits of vote counts.

In order to audit their vote counts and monitor the accuracy of vote counting systems, all state and county election offices should set up election data reporting systems to quickly and easily make publicly available, their precinct-level vote totals, broken out by vote type (i.e. election day, absentee, overseas, provisional, early voting, etc.) If vote counts are not reported down to this detailed level, then padded votes in one vote type can easily "cancel out" under-votes in another type. In other words votes can be subtracted from one candidate in one vote type, while being added for another candidate in another vote type, yet these two problems, when added together, may look perfectly normal.

The Future: How would a National Election Data Archive Protect Democracy?

If, for decades, we had never independently audited our financial institutions, we would expect to see ubiquitous insider embezzlement of monies. For decades now, we have counted the vast majority of U.S. votes via mechanical or electronic methods, yet there have never been any routine independent audits of vote counts.
US Count Votes is seeking funding to create the first-ever nation-wide database of precinct-level and vote-type election results in order to statistically audit U.S. vote counts to detect patterns that suggest the embezzlement of votes. To obtain all the needed election data in all its diverse forms from the over 33,000 separate election offices in America is a huge project. Full-time programming staff, statisticians, and administrative staff are needed. For somewhat less than one million dollars, the National Election Data Archive could assist all candidates of any party to determine whether or not their elections were accurately counted, and produce court-worthy evidence that is needed to obtain recounts, investigations, or possibly even re-elections.

The "National Election Data Archive" project is particularly important, given the fact that private exit pollsters could, in the future, elect to adjust exit poll data to conform to actual official election results and neglect to publicly release any "unadjusted" exit poll data. The development of a "National Election Data Archive" would provide the public with all the data it needs to analyze vote counts within days of the November 2006 election. The technical implementation of well-developed and sound plans for such a system needs to begin very soon, in order to ensure by January 2007 and thereafter, that the candidates actually selected by the voters, are sworn into office. Our hope is that through careful analysis, we can develop the capacity to identify future vote count errors, whether fraudulent or inadvertent, in time to challenge the outcomes. "

THIS, MY FELLOW CITIZENS, IS WHAT MUST BE DONE. ANYTHING LESS WILL BRING GREATER SUFFERING TO ALL OF US AND THE WORLD.

NO DIEBOLD ELECTRONIC VOTING MACHINES IN CALIFORNIA!

We the undersigned oppose the use of Diebold Electronic Voting machines in California. There is strong reason to believe that the Diebold company may have "delivered" Ohio and other states to George Bush (to use the words of Diebold's CEO at a Bush fundraiser.) Statisticians from around the country have calculated that the probability of random error in the exit polls from precincts that favored Kerry but ending up "voting" for Bush are 1 million to 1. The Bush administration, in typical hypocritical fashion, used exit polls as a basis for calling the Ukrainian Election fraudulent, whereas they deemed exit polls "wrong" in the 2004 presidential election.

So far, Diebold has not allowed the software of their machines to be inspected by non-partisan experts to see if there were glitches in the programming or if the machines were deliberately programmed to favor Bush. They hide behind patent protection laws. Until there is a complete, impartial investigation of the Diebold machines and the company's impact on the results of the 2004 election, no further contracts should be awarded to Diebold. Indeed, if the suspicions of a large number of American voters are proven correct, jail sentences for those responsible for the alleged stealing of the 2004 election would be more appropriate.

	Name	Address	City	Phone
1.	Jonathan Simonoff	373 Chenery St.	San Francisco	415-337-7917
2.	Lorene K. Reed	111 Fetters Ave	Sonoma CA.	707-933-3867
3.	Rosemary Sabino-Blodget	1562 Mt. View Ave.	Chico, CA	530-345-1922
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				

NO DIEBOLD ELECTRONIC VOTING MACHINES IN CALIFORNIA!

We the undersigned oppose the use of Diebold Electronic Voting machines in California. We believe Diebold company may have stolen the elections of 2004 and 2002. If so, those responsible deserve prison sentences, not a contract with the State of California.

Name **Address** **Phone**

1. Robert Bowman 12 Stansbury Ct Chico 95928 (530)521-2578
2. Laura Gilpin 227 W. 3rd Ave. Chico 95926 530 520-8239
3. [illegible] Bradshaw POB 474 Forest Ranch 95942 530-892-1917
4. [illegible] 6060 El Moreno St 530-521-8903
5. [illegible] 1197 Honey Run Rd Chico CA 95928
6. Michael [illegible] 1358 E. 10th St. Chico 95928
7. Margaret Swick 144 Copperfield Chico 95928
8. Ken Coyle 187 E 11th St. Chico, 95928
9. Jeff Johnson 1118 Nord Ave #73 95926
10. Judy Kane 12 Stansbury Ct Chico CA 95928 530-893-3705
11. [illegible] S. Jackson, 2 Stansbury Ct. 95928
12. Agatha F. Jones 2 Stansbury Ct. Chico, CA 95928
13. Alina Neacy PO Box 95927-0652 (650) 279-5431
14.
15.
16.
17.
18.
19.
20.

Voter Confidence Resolution

v6.1, LAST UPDATED: 5/3/05 1AM

http://guvwurld.blogspot.com

Whereas an election is a competition for the privilege of representing the people; and

Whereas each voter is entitled to cast a single ballot to record his or her preferences for representation; and

Whereas the records of individual votes are the basis for counting and potentially re-counting a collective total and declaring a winner; and

Whereas an election's outcome is a matter of public record, based on a finite collection of immutable smaller records; and

Whereas a properly functioning election system should produce unanimous agreement about the results indicated by a fixed set of unchanging records; and

Whereas recent U.S. federal elections have been conducted under conditions that have not produced unanimous agreement about the outcome; and

Whereas future U.S. federal elections cannot possibly produce unanimous agreement as long as any condition permits an inconclusive count or re-count of votes; and

Whereas inconclusive counts and re-counts have occurred during recent U.S. federal elections due in part to electronic voting devices that do not produce a paper record of votes to be re-counted if necessary; and

Whereas inconclusive results have also been caused by election machines losing data, producing negative vote totals, showing more votes than there are registered voters, and persistently and automatically swapping a voter's vote from his or her chosen candidate to an opponent; and

Whereas inconclusive results make it impossible to measure the will of the people in their preferences for representation; and

Whereas the Declaration of Independence refers to the Consent of the Governed as the self-evident truth from which Government derives "just Power";

THEREFORE BE IT RESOLVED:

Because inconclusive results, by definition, mean that the true outcome of an election cannot be known, there is no basis for confidence in the results reported from U.S. federal elections; and

Be it also resolved:

The following is a comprehensive election reform platform likely to ensure conclusive election results and create a basis for confidence in U.S. federal election:

1) voting processes owned and operated entirely in the public domain, and
2) clean money laws to keep all corporate funds out of campaign financing, and
3) a voter verifiable paper ballot for every vote cast and additional uniform standards determined by a non-partisan nationally recognized commission, and
4) declaring election day a national holiday, and
5) counting all votes publicly and locally in the presence of citizen witnesses and credentialed members of the media, and
6) equal time provisions to be observed by the media along with a measurable increase in local, public control of the airwaves, and
7) presidential debates containing a minimum of three candidates, run by a non-partisan commission comprised of representatives of publicly owned media outlets, and
8) preferential voting and proportional representation to replace the winner-take-all system for federal elections;

Be it further resolved:

When elections are conducted under conditions that prevent conclusive outcomes, the Consent of the Governed is not being sought. Absent this self-evident source of legitimacy, such Consent is not to be assumed or taken for granted.

* * *

To endorse the Voter Confidence Resolution or schedule a presentation, contact blog@guvwurld.org.

http://guvwurld.blogspot.com • http://www.guvwurld.org

http://www.voterconfidencecommittee.org